Norton™ Internet Security

Product Manual

Care for our Environment, 'It's the right thing to do'.
Symantec has removed the cover from this manual to reduce the Environmental Footprint of our products. This manual is made from recycled materials.

Norton™ Internet Security Product Manual

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 19.0

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Norton, SONAR, LiveUpdate, Norton AntiSpam, Norton AntiVirus, Norton Internet Security, Norton 360, and Norton SystemWorks are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Windows is a trademark of Microsoft Corporation. Portions of this product Copyright [1996-2008] Glyph & Cog, LLC. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Norton License Agreement
Norton™ Internet Security

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT") CAREFULLY BEFORE USING THE SOFTWARE (AS DEFINED BELOW). SYMANTEC CORPORATION, IF YOU ARE LOCATED IN THE AMERICAS; OR SYMANTEC ASIA PACIFIC PTE LTD, IF YOU ARE LOCATED IN THE ASIA PACIFIC RIM OR JAPAN; OR SYMANTEC LIMITED, IF YOU ARE LOCATED IN EUROPE, THE MIDDLE EAST OR AFRICA ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "I AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "CANCEL" OR "NO" OR "CLOSE WINDOW" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT YOUR VENDOR OR SYMANTEC CUSTOMER SERVICE, USING THE CONTACT DETAILS IN SECTION 10 OF THIS LICENSE AGREEMENT, FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES EXCEPT IN CERTAIN STATES AND COUNTRIES WHERE SHIPPING, HANDLING, AND TAXES ARE REFUNDABLE) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software (including any accompanying features and services) and documentation (including any product packaging) (the "Documentation"), that accompanies this License Agreement (collectively the "Software") is the property of Symantec or its licensors, and is protected by copyright law. Although Symantec continues to own the Software, after Your acceptance of this License Agreement You will have certain rights to use the Software during the Service Period. The "Service Period" shall begin on the date of Your initial installation of the Software on a computer, mobile or mobile computing device (a "Device"), regardless of the number of copies that You are permitted to use in accordance with Section 1.A of this License Agreement, and shall last for the period of time set forth in the Documentation or the applicable transaction documentation from the authorized distributor or reseller from which You obtained the Software. The Software may automatically deactivate and become non-operational at the end of the Service Period, and You will not be entitled to receive any feature or content updates to the Software unless the Service Period is renewed. Subscriptions for renewals of the Service Period will be available in accordance with Symantec's support policy posted at

http://www.symantec.com/norton/support/technical_support_policy.jsp.

This License Agreement governs any releases, revisions, updates or enhancements to the Software that Symantec may make available to You. Except as may be modified by the Documentation, and subject to Symantec's right to terminate for Your breach pursuant to Section 9, Your rights and obligations under this License Agreement with respect to the use of this Software are as follows.

During the Service Period, You may:

A.use one copy of the Software on a single Device. If a greater number of copies and/or number of Devices is specified within the Documentation or the applicable transaction documentation from the authorized distributor or reseller from which You obtained the Software, You may use the

Software in accordance with such specifications;

B. make one copy of the Software for back-up or archival purposes, or copy the Software onto the hard disk of Your Device and retain the original for back-up or archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each Device that can access the Software over that network;

D. permanently transfer all of Your rights in the Software granted under this License Agreement to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this License Agreement. Partial transfer of Your rights under this License Agreement shall not be permitted. For example, if the applicable documentation grants You the right to use multiple copies of the Software, only a transfer of the rights to use all such copies of the Software would be valid; and

E. use the Software in accordance with any additional permitted uses which may be set forth below.

You may not, nor may you permit any other person to:

A. sublicense, rent or lease any portion of the Software;

B. reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider or service bureau arrangement; or

D. use the Software in any manner that is not permitted pursuant to this License Agreement.

2. Software Feature and Content Updates:

A. You shall have the right to receive new features to the Software as Symantec, in its sole discretion, makes such features available with the Software during Your Service Period. Symantec continually strives to improve the usability and performance of its products and services. In order to optimize the Software Symantec may, at its discretion and without notice, add, modify or remove features from the Software at any time.

B. Certain Software uses content that is updated from time to time, including but not limited to the following Software: antivirus and crimeware software use updated virus definitions; antispyware software uses updated spyware definitions; antispam software uses updated antispam rules; content filtering and antiphishing software use updated URL lists; some firewall software use updated firewall rules; vulnerability assessment products use updated vulnerability data and web site authentication software uses updated lists of authenticated web pages; these updates are collectively referred to as “Content Updates” (or alternatively referred to as “Protection Updates” or “Security Updates” at times). You shall have the right to receive Content Updates for the Software during Your Service Period.

3. Product Installation; Required Activation:

A. During the installation process, the Software may uninstall or disable other security products, or features thereof, if such products or features are incompatible with the Software or for purposes of improving the overall functionality of the Software.

B. There may be technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a Device to not more than a finite number of times for a finite number of Devices. This License Agreement and the Software containing enforcement technology may require activation as further set forth in the Documentation. If so, the Software will only operate for a finite period of time prior to Software activation by You. During activation, You may be required to provide Your unique activation code accompanying the Software and Device configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation, or as prompted

by the Software, the Software will cease to function until activation is complete; at which time the Software functionality will be restored. In the event that You are not able to activate the Software over the Internet, or through any other method specified during the activation process, You may contact Symantec Customer Support using the information provided by Symantec during activation, or as set forth below.

5. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please make no further use of the Software and contact Symantec Customer Service, using the contact details set out in Section 10 of this License Agreement, for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes except in certain states and countries where shipping, handling and taxes are refundable) at any time during the sixty (60) day period following the date of purchase.

6. Limited Warranty:

Symantec warrants that any media manufactured by Symantec on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

7. Disclaimer of Damages:

SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE WHICH YOU PAID FOR THE APPLICABLE SERVICE PERIOD. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

8. U.S. Government Restricted Rights:

For U.S. Government procurements, the Software is deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Software by the U.S. Government shall be solely in accordance with the terms of this License Agreement.

9. Export Regulation:

You acknowledge that the Software and related technical data and services (collectively "Controlled Technology") may

be subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. You agree to comply with all relevant laws and will not export any Controlled Technology in contravention to U.S. law nor to any prohibited country, entity, or person for which an export license or other governmental approval is required. All Symantec product is prohibited for export or re-export to Cuba, North Korea, Iran, Syria and Sudan and to any country subject to relevant trade sanctions. USE OR FACILITATION OF SYMANTEC PRODUCT IN CONNECTION WITH ANY ACTIVITY INCLUDING, BUT NOT LIMITED TO, THE DESIGN, DEVELOPMENT, FABRICATION, TRAINING, OR TESTING OF CHEMICAL, BIOLOGICAL, OR NUCLEAR MATERIALS, OR MISSILES, DRONES, OR SPACE LAUNCH VEHICLES CAPABLE OF DELIVERING WEAPONS OF MASS DESTRUCTION IS PROHIBITED, IN ACCORDANCE WITH U.S. LAW.

10. General:

This License Agreement will be governed by the laws of the State of California, United States of America. This License Agreement is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. Notwithstanding the foregoing, nothing in this License Agreement will diminish any rights You may have under existing consumer protection legislation or other applicable laws in Your jurisdiction that may not be waived by contract. This License Agreement shall terminate upon Your breach of any term contained in this License Agreement and You shall cease use of and destroy all copies of the Software and Documentation. The disclaimers of warranties and damages and limitations on liability shall survive termination. This License Agreement may only be modified by the Documentation or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this License Agreement, or if You desire to contact Symantec for any reason, please write to Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or visit the Support page at t www.symantec.com.

ADDITIONAL TERMS AND CONDITIONS

Your use of the Software is subject to the terms and conditions below in addition to those stated above.

11. Privacy; Data Protection:

From time to time, the Software may collect certain information from the Device on which it is installed, which may include:

Information on potential security risks as well as URLs of websites visited that the Software deems potentially fraudulent. The URLs could contain personally identifiable information that a potentially fraudulent website is attempting to obtain without Your permission. This information is collected by Symantec for the purpose of delivering the functionalities of the software, and also for evaluating and improving the ability of Symantec's products to detect malicious behavior, potentially fraudulent websites and other Internet security risks. URLs of websites visited as well as search keywords and search results only if the Norton Safe Web feature is enabled. This information is collected by Symantec for the purpose of providing protection and of evaluating and advising You regarding potential threats and risks that may be associated with a particular Web site before You view it.

Executable files and files that contain executable content that are identified as potential malware, including information on the actions taken by such files at the time of installation. These files are submitted to Symantec using the Software's automatic submission function. The collected files could contain personally identifiable information that has been obtained by the malware without Your permission. Files of this type are being collected by Symantec only for the purpose of improving the ability of Symantec's products to detect malicious behavior. Such automatic submission function may be deactivated after installation by following the instructions in the Documentation for applicable products.

The name given to the Device during the initial setup of such Device. If collected, the name will be used by Symantec as an account name for the Device under which You may elect to receive additional services and/or under which You may use certain features of the Software. You may change such account name at any time after installation of the Software (recommended).

Status information regarding installation and operation of the Software. This information indicates to Symantec whether installation of the Software was successfully completed as well as whether the Software has encountered an error. The status information could contain personally identifiable information only if such information is included in the name of the file or folder encountered by the Software at the time of installation or error. The status information is collected by Symantec for the purpose of evaluating and improving Symantec's product performance and installation success rate. Symantec may also use this information to optimize its web-pages.

Information contained in email messages that you send through the Software to Symantec to report as spam or as incorrectly identified as spam. These email messages may contain personally identifiable information and will be sent to Symantec only with your permission, and will not be sent automatically. If you send such messages to Symantec, Symantec will use them only for the purpose of improving the detection ability of Symantec's antispam technology. Symantec will not correlate these files with any other personally identifiable information.

Information contained in a report that You may choose to send through the Software to Symantec when the Software encounters a problem. The report includes information regarding the status of both the Software and Your Device at the time that the Software encountered the problem. The status information about Your Device may include the system language, country locale, and the operating system version for Your Device, as well as the processes running, their status and performance information, and data from files or folders that were open at the time the Software encountered the problem. The information could contain personally identifiable information if such information is included in, or is a part of the name of the files or folders open at the time the Software encountered the problem. This information will be sent to Symantec only with Your permission, and will not be sent automatically. The information is collected by Symantec for the purpose of correcting the encountered problem and improving Symantec's product performance. This information will not be correlated with any personally identifiable information.

The Internet Protocol (IP) address and/or Media Access Control (MAC) address and the Machine ID of the computer on which the Software is installed to enable the Software to function and for license administration purposes.

Other general, statistical information used for product analysis, and for improving product functionality.

Unless it is expressly defined as optional, the collected information as set out above is necessary for the purpose of the functionality of Symantec's products.

Information may be transferred to the Symantec group in the United States or other countries that may have less protective data protection laws than the region in which You are situated (including the European Union) and may be accessible by Symantec employees or contractors exclusively to be used in accordance with the purposes described above. For the same purposes the information may be shared with partners and vendors that process information on behalf of Symantec. Symantec has taken steps so that the collected information, if transferred, receives an adequate level of protection.

Subject to applicable laws, Symantec reserves the right to cooperate with any legal process and any law enforcement or other government inquiry related to your use of this Software. This means that Symantec may provide documents and information relevant to a court subpoena or to a law enforcement or other government investigation. In order to promote awareness, detection and prevention of Internet security risks, Symantec may share certain information with research organizations and other security software vendors. Symantec may also use statistics derived from the information to track and publish reports on security risk trends. By using the Software, You acknowledge and agree that Symantec

may collect, transmit, store, disclose and analyze such information for these purposes.

CPS / S 5.0 / USE

Contents

Chapter 1 Getting started 13
Activation protects you 13
About Norton Internet Security main window 17
About your Norton Account 33
About Norton Community Watch 39
About Norton Bootable Recovery Tool 41
Starting Norton Internet Security from the command prompt 46
About the Norton Internet Security icon 46
About LiveUpdate 49
About Network Proxy settings 60

Chapter 2 Monitoring your system's performance 65
About System Insight 65

Chapter 3 Protecting your files and data 107
About maintaining protection 107
About the Norton Internet Security scans 110

Chapter 4 Responding to security issues 179
What to do if a security risk is found 179

Chapter 5 Protecting Internet activities 193
About the Smart Firewall 193
About Download Insight 233
About Intrusion Prevention 244
About Vulnerability Protection 251
About the types of security risks 254
About Norton AntiSpam 255
About configuring POP3 and SMTP ports 269
About the Network Security Map 272
About Metered Broadband Mode 297

Chapter 6 Securing your sensitive data 301
About securing your sensitive data 301

Chapter 7 Monitoring protection features 371
About Security History 371

Chapter 8 Customizing protection features 407
Feature summary 407
About turning off automatic features 416
About customizing settings and options 422

Chapter 9 Finding additional solutions 473
Finding the version number of your product 473
Finding the End-User License Agreement 474
About upgrading your product 474
About Norton Autofix 477
Staying informed about protection issues 479
About Support 481
About uninstalling 486

Index 491

Getting started

1

This chapter includes the following topics:

- Activation protects you
- About Norton Internet Security main window
- About your Norton Account
- About Norton Community Watch
- About Norton Bootable Recovery Tool
- Starting Norton Internet Security from the command prompt
- About the Norton Internet Security icon
- About LiveUpdate
- About Network Proxy settings

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software. It protects you by limiting the use of a product to those users who have acquired the product legitimately. Product activation requires a product key for each installation of a product. You must activate the product within a limited time period after you install it.

If you are connected to the Internet, product activation takes place automatically when you start the product for the first time after installation. After activation, the **Norton Account** window appears. You can create your Norton Account and register your product.

If you are not connected to the Internet, you can click **Try Later** in the **Activation not complete** window to start your product. The **Activation** window reappears every time you start your product until you activate your product. If you choose not to activate at that time, you receive an alert that reminds you to activate the product. You can also activate your product from the Norton Internet Security main window.

If you do not activate the product within the time period that the alert specifies, the product stops working. You can activate it after the time period has elapsed, but you are not protected until you activate the product.

Activating your product

If you did not activate your product during installation, you receive an activation-needed alert regularly until you activate the product.

Product activation reduces software piracy and ensures that you use authentic Symantec software. Activation provides you with a specified period of subscription to your Norton product. You can also renew your subscription to continue using Norton Internet Security.

You must activate your product within the time period that the alert specifies, or your product stops working.

You can activate your product directly from the activation-needed alert or from the main window. Activation should take only a few minutes.

During activation, the **Norton Account** window appears. You can create your Norton Account and register your product. You can also view details, such as your product key, your registration date, and recent

updates to the product. If you skip the **Norton Account** window, the product is activated, but the product key is not saved in the Norton Account. You can print the product key to reinstall your product in the future.

To activate your product from the alert

1. In the alert, do one of the following:
   - If you purchased a subscription version of a retail product or the product came installed on your computer, select **Activate Now (Recommended)**.
   - If you want to renew the subscription of your product, select **Renew Now**.

   You can also activate or renew the subscription of your product from any non-admin user account.
2. Click **OK**.
3. Follow the on-screen instructions to activate or renew your product.
4. In the window that appears, click **Done**.

To activate your product from the main window

1. In the Norton Internet Security main window, do one of the following:
   - If you purchased a subscription version of a retail product, click **Activate Now**.
   - If the product came installed on your computer, click **Activate Online Now**.
   - If you want to renew the subscription of your product, click **Renew**.

   You can also activate or renew the subscription of your product from any non-admin user account.
2. Follow the on-screen instructions to activate or subscribe your product.
3. In the window that appears, click **Done**.

Where to find your product key

The product key is a unique key that helps you to install and activate the Symantec product on your computer.

The product key is a 25-character alphanumeric string that is shown in five groups of five characters each, separated by hyphens. The location of the product key varies depending on how you acquired the product.

The locations of the product key are as follows:

If you purchased a retail copy of the product on CD	The product key is either on a sticker on the CD sleeve or on an insert in the product package.
If you purchased the product on DVD	The product key is on the DVD package.
If you downloaded the product from the Symantec Store	The product key is stored on your computer as part of the download process and is included in the confirmation email from the Symantec Store.
If your computer came with the product already installed	The product key is provided as part of the activation process. Be sure to save your product key by creating or signing in to your Norton Account, or by printing the key. You may need the product key if you ever want to reinstall your product.
If you received a product key card	The product key is printed on the card along with instructions on how to use it. Be sure to save your product key by creating or signing in to your Norton Account. You need the product key if you ever want to reinstall the product.

If you are still unable to locate your product key, you can recover it using Norton Account	To recover or access your product key log on to https://www.mynortonaccount.com. If you are not registered, register for Norton Account. You can find the product key on the **Products** tab in the **Norton Account** page.

About problems during activation

If you cannot connect to the Symantec servers to activate your product, first check your Internet connection. You then need to see if you have parental control software, either installed or through your ISP, that might block the connection.

A connectivity problem can occur if you use parental control software. If you suspect that parental controls might block the connection, you can configure the parental controls so that they do not block the activation procedure. You need to log in to your parental control software or to the Internet through your ISP as an administrator to change your configuration.

If you use a proxy server to connect to the Internet, you must configure the proxy settings. To use the **Proxy Server** option, go to the Norton Internet Security main window, and then click **Settings > Network > Network Security Settings > Proxy Server > Configure**.

About Norton Internet Security main window

The Norton Internet Security main window acts as a security management interface. You can access the main features and monitor the performance of your computer from the main window.

You can find the following items in the main window:

System Status	Lets you view the overall protection status of your computer. When your system status is **Secure**, your computer is fully protected. When your system status is at **Attention** state, ensure that you fix all the issues. When your system status is at **At Risk** state, you must take immediate actions to fix the issues.
Settings	Lets you access the **Settings** window. You can view and configure various options to customize the Norton Internet Security settings.
Performance	Lets you access the **Performance** window. The **Performance** window displays a chronicle representation of all the installs, downloads, optimizations, detections, alerts, and instances of Quick Scan. The window also displays a detailed graphical representation of CPU and memory usage by your Norton product.

Feedback	Lets you provide feedback on the product on a Symantec Web page. This feature may not be available in some versions of Norton Internet Security.
Account	Lets you create or access your Norton Account. Norton Account lets you manage all of your Norton products in one place. This feature may not be available in some versions of Norton Internet Security.
Support	Lets you access the **Norton Autofix** window that provides you various support options. You can also access the online Help from the **Support** drop-down menu. Help provides links to information that assists you with the specific tasks that you want to complete. The online Help guides you to configure all of the product features. You can also access the product's version number.

You can use the following options to perform the important tasks in Norton Internet Security:

Scan Now	Lets you access different types of scans to protect your computer and your sensitive data. By using the Scan Now option, you can run the following types of scans: ▪ **Computer Scan** Lets you run different computer scans including **Quick Scan**, **Full System Scan**, and **Custom Scan**. ▪ **Reputation Scan** Lets you run different reputation scans including **Quick Scan**, **Full System Scan**, and **Custom Scan**. ▪ **Scan Facebook Wall** Lets you scan News Feeds on your Facebook Wall periodically to protect you from malicious links.
LiveUpdate	Lets you run LiveUpdate to download the latest virus definitions and program updates. Norton Internet Security uses the latest virus definitions from Symantec servers to detect and remove latest security threats.

Advanced	Lets you access the Norton Internet Security advanced window. By using the Norton Internet Security advanced window, you can do the following: ▪ Run different scans. ▪ View Security History. ▪ View the quarantined items in the **Security History** window. ▪ View Norton Insight - Application Ratings. ▪ View the list of programs that are vulnerable on your computer and find how Norton protects you from the program vulnerabilities. ▪ View and configure Network Security Map. ▪ Manage logins and cards. ▪ Configure parental controls. In addition, you can choose to turn on or turn off the protection features from this window.

The bottom section of the Norton Internet Security main window provides you up-to-date virus and threat information. When your system status is **At Risk** or **Attention**, this section automatically provides you the **Fix Now** option to fix all the issues at once.

The bottom section of the Norton Internet Security main window helps you do the following:

Activity Map

Lets you access the world map with hotspots of cybercrimes and the latest threats.

The Activity Map shows the top cities in the world where most of the cybercrime activities occur. These cities are represented as yellow dots on the map. You can click a continent in the world map to view its cities with the highest number of threats. The details on the Activity Map are updated from a Symantec server on a regular basis. Your computer must be connected to the Internet to receive the activity map updates.

You can view the date and time that the Activity Map was last updated. You can also use the **Details** link to get a brief idea of the Activity Map.

When you click **Details**, the Activity Map shows a series of latest viruses and threats that your product protects your computer from. You can use the **info** link next to each item to view its details in an overlay window. You can also use the **View Details** link in the overlay window to know more about the threat in a Symantec Web page.

Online Family

Lets you monitor your child's activities on the Internet.

Norton Online Family may not be available in some versions of Norton Internet Security.

When you click the **Online Family** icon on the main window, the bottom section of the Norton Internet Security main window displays Norton Online Family sign in options. Norton Online Family provides you advanced controls to monitor your child's online activities.

You can use the link on the bottom section of the Norton Internet Security main window to set up your account with Norton Online Family.

Symantec recommends that you use your Norton Account login credentials to sign in to Norton Online Family. If you register your product with your Norton Account, your Norton Account email address is auto-filled in the email address text box.

After you set up your account, you can sign in to your account on the bottom section of the Norton Internet Security main window and view your child's Internet activities. The bottom section of the Norton Internet Security main window shows

	details such as your child's latest search terms, and the latest alerts. After you sign in, you can use the **Get Details** option in the bottom section of the Norton Internet Security main window to view more details on the Norton Online Family Web site.
Manage	Lets you access Norton Management. Norton Management lets you manage your Norton products on all of your devices from one location. Click the **Manage** icon at the bottom of the main window to sign up for or log into Norton Management. The Norton Management agent should be installed on each device that you want to add to Norton Management. You can use your existing Norton Account login information to access Norton Management. Norton Management may not be available in some versions of Norton Internet Security.

Mobile	Lets you download the Norton Mobile Security for Android. You can use Norton Mobile Security on all your devices that use Android operating system. Norton Mobile Security may not be available in some versions of Norton Internet Security.
Backup	Lets you set up the Norton Online Backup account or access your online backup status. Norton Online Backup may not be available in some versions of Norton Internet Security. When you click the **Backup** icon on the main window, the bottom section displays Norton Online Backup options. Norton Online Backup provides a secure online backup solution that safeguards your important data against system crash, accidental deleting, virus infection, and other disasters. You can access or restore the backed up data from any computer that is connected to the Internet.

Safe Web

Lets you check the safety of a Web site.

You can also perform a safe search.

This option may not be available with some versions of Norton Internet Security.

When you click the **Safe Web** icon on the main window, the bottom section of the Norton Internet Security main window displays Norton Safe Web options.

You can use the **Check Site** option in the bottom section of the Norton Internet Security main window to analyze the security levels of any Web site that you want to visit. When you type a Web site address in the text box and click **Check Site**, it shows the Symantec's ratings for the Web site.

You can use the **Safe Search** option in the bottom section of the Norton Internet Security main window to search for information on the Internet. The Norton Safe Search uses Ask.com to generate the search results. Norton Safe Search provides a site safety status and a Norton rating for each of the search results generated.

You can also use the **View recent Norton Safe Web activity** option in the bottom

section of the Norton Internet Security main window to view the recent Norton Safe Web statistics on malicious sites and URLs. You can also view the list of new malicious URLs.

Your activation status or subscription status appears at the bottom of the main window. You can use the **Activate Now** option to activate or subscribe your Norton product.

About the Norton Internet Security advanced window

The Norton Internet Security advanced window acts as a security management interface. The options in this window help you address all the important security and performance issues of your computer. The options are classified in different panes. Each pane contains the important features that you can easily access or configure from this window.

The panes are:

Computer Protection	Provides you the essential computer protection options. It also contains links to scan your computer, view the history of protection events, and manage quarantined items. You can also view the **Norton Insight - Application Ratings** window and improve the performance of Norton Internet Security scans. In addition, you can run LiveUpdate. It also displays the updates availability as to when the last virus definitions were updated.
Network Protection	Provides you the essential network protection options. It also contains links to the list of vulnerable programs and Network Security Map.
Web Protection	Provides you the essential Web protection options. It also contains links to managing logins and credit cards. In addition, you can monitor and manage the computer usage and Internet activities of your child. The parental control feature is not available in some of the versions of Norton Internet Security.

You can view the different protection features on the right side of the window. You can move your mouse pointer over each feature to view a brief summary about the feature. You can also choose to ignore or monitor the protection status of a feature. You can choose to turn on or turn off the protection features from this window.

You can also monitor the overall system CPU usage and the Norton-specific CPU usage in this window.

Responding to System Status indicators

Norton Internet Security displays the overall protection status of your computer as **System Status** at the top of the main window. When the **System Status** needs attention or is at risk, you can take appropriate action to improve the **System Status**. Your computer protection is based on the programs that are installed on your computer. To improve your protection status, ensure that your installed programs are up to date.

The **System Status** indicator displays the following statuses:

Secure	Indicates that your computer and activities are protected from threats, risks, and damage.
Attention	Indicates that your computer and activities require attention. Take appropriate action to improve your protection status.
At Risk	Indicates that your computer and activities are at risk. Take immediate action to improve your protection status.

You can respond to the **System Status** indicators directly from the main window.

To respond to System Status indicators from the main window

1. In the bottom section of the Norton Internet Security main window, click **Fix Now**.
2. Follow the on-screen instructions.

Monitoring the protection status of a feature

The Norton Internet Security main window acts as a security management interface. You can access the main features and monitor the performance of your computer from the main window.

At times, you may want to turn off any option for a particular purpose. But by doing so, the status of your system changes to **Attention** or **At Risk**. In such cases, you can ignore the protection status of a particular feature to maintain a healthy overall system status. For example, you want to turn off **Browser Protection** for a limited period, and you still want the system status to be **Secure**. In this case, you can ignore the protection status of **Browser Protection** and then, turn off the option. When you ignore the protection status of a feature, it does not affect the overall **System Status**.

You can also monitor the protection status of the feature that has been ignored at any time.

You can ignore or monitor the protection status of only selected features that are available in the main window.

The features are:

- Antivirus
- Antispyware
- SONAR Protection
- Smart Firewall
- Intrusion Prevention
- Email Protection

- Browser Protection
- Safe Surfing

To monitor the protection status of a feature

1. In the Norton Internet Security main window, click **Advanced**.
2. In the window that appears, move your mouse pointer over the feature name.
3. In the pop-up that appears, do one of the following:
   - To ignore the protection status of the feature that affects your computer's overall health evaluation, click **Ignore**.
   - To monitor the protection status of the feature that has been ignored, click **Monitor**.

About your Norton Account

When you create a Norton Account, you can manage all of your Norton products in one place. You can store your product keys in your Norton Account and also buy additional product keys. You can also register your product with the Norton Account. It takes only a few moments to create your Norton Account. You must be connected to the Internet to create a Norton Account.

After you create a Norton Account, you can access and manage your account information and product information from anywhere. It helps to reinstall your products and download the latest version of the products. If you install your product on more than one PC, you can use the same Norton Account. To access your Norton Account, go to the following URL:

https://www.mynortonaccount.com

You can create a Norton Account in the following ways:

- During activation

  You can create your Norton Account and register your product from the **Norton Account** window that appears when you activate the product. You

must provide your account information in the **Norton Account** window that appears.

- Any time after activation

  If you skip the **Norton Account** window during activation, you can create a Norton Account any time after activation. You can create your Norton Account and register your product from the **Account** link that appears at the top of the Norton Internet Security main window.

After you log in to your Norton Account, you can manage your product information with the following options:

Products	Saves the information for all of the Norton products that you own. The **Products** tab provides you the information about the Norton products that you own and the expiration date. You can click the arrow icon against a product for more information such as product key and the registration date. You can also buy a new product key to protect additional computers. You can use the **Update** option to check and download the latest product version using Norton Update Center.
Order History	Contains order information of the Norton products you bought from Norton online store.

Profile	Saves your account information and your billing details. The **Profile** options are: ▪ **Account Information** You can update your Norton Account information and your shipping address on the **Account Information** tab. After you update, click **Update** to save the changes. ▪ **Billing Information** You can save your credit card information and your billing address on the **Billing Information** tab. It makes it easier for saving online orders. After you update, click **Update** to save the changes. ▪ **Change Password** You can change your current Norton Account password on the **Change Password** tab.

You can use the icons at the bottom of your Norton Account Web page to access and use the following:

Norton Online Family	Norton Online Family monitors and manages your child's Internet activities and computer usage.

Norton Online Backup	Norton Online Backup provides a secure and easy-to-use online backup solution that safeguards your important data against system crash, accidental deleting, virus infection, and other disasters.
Norton Safe Web	Norton Safe Web checks the safety of a Web site and lets you perform a safe Web search.
Norton.com	The Symantec Web site provides more information about the various products of Symantec, the latest updates on Internet security, and various support options.
Norton Update Center	Norton Update Center checks and lets you download the latest version of your Norton product.

If you forget your Norton Account password, you can get a temporary password by clicking the **Forgot your password** link in the **Norton Account** sign-in Web page. You need to provide your email address. You need to use the same email address that you provided when you created your Norton Account. Symantec sends a temporary password to your email address. You can use the temporary password for a limited time period. You must reset your password after you log in to your Norton Account.

Creating a Norton Account

Your Norton Account stores the product key and the billing information of your product. You can also register your product with the Norton Account.

In addition, Norton Account helps you to do the following:

- Access the product key and other product information when you need it.
- Reinstall your Norton product.
- Buy additional product keys for your home or office.
- Check and download the latest version of the product by using Norton Update Center.
- Save online orders and update billing information.
- Log in to other product add-ons such as Norton Online Family and Norton Online Backup.

Your computer must be connected to the Internet to create a Norton Account. If you use a proxy server to connect to the Internet, you must configure the proxy settings. To configure the proxy settings of your network, go to the Norton Internet Security main window, and then click **Settings > Network > Network Security Settings > Proxy Server > Configure**.

You can also create a Norton Account when you activate your product. When you create your Norton Account from the product, your product gets registered in your account. If you have an existing Norton Account, you can provide the same email address in the **Norton Account** window in your product. This way, you can register your current product and add it to the list of Norton products in your existing Norton Account. If you upgrade your registered product to the latest available version, your product remains registered to the same Norton Account. In this case, you can continue using the same Norton Account login credentials.

Symantec products that are older than the 2006 product year do not appear in your Norton Account.

To create a Norton Account from the Norton Account Web page

1. In the Norton Internet Security main window, click **Account**.
2. In the Norton Account Web page that appears, click **Sign up now**.
3. In the **Norton Account Sign Up** Web page, provide the details about your account information, and then click **Sign Up**.

To create a Norton Account and register your product after activation

1. In the Norton Internet Security main window, click **Account**.
2. In the **Complete Your Activation** window, type your email address, and then click **Next**.
3. In the **Create your Norton Account** window, provide your account details, and then click **Next**.
   Your product information gets saved in your Norton Account only after you log in to your Norton Account.
4. In the window that appears, click **Done**.

To log in to your Norton Account and access your product information, visit https://www.mynortonaccount.com.

Accessing your Norton Account

The product key for each Norton product is conveniently stored in your Norton Account. After you have created your Norton Account successfully, you can access your account from anywhere in the world. You can log in to your Norton Account any time by visiting the following URL:

https://www.mynortonaccount.com

You can easily find and update your account, product, and billing information from your Norton Account. You can also change your Norton Account password,

if required. Your computer must be connected to the Internet to access your Norton Account.

Symantec products that are older than the 2006 product year do not appear in your Norton Account.

To access Norton Account

1. In the Norton Internet Security main window, click **Account**.
2. In the Web page that appears, type your email address and password, and click **Sign In**.

About Norton Community Watch

Norton Community Watch helps in identifying new security risks by submitting selected security and application data to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. The collective efforts from Norton security product users help in quick identification of solutions for these threats and risks. Norton Community Watch improves user security and product functionality. In addition, it helps Symantec to analyze the execution, schedule, and efficiency of Norton-specific tasks and settings on your computer.

Norton Community Watch collects and submits the following types of data:

- Identified malicious software such as portable executable files and running processes
- Any Web site URL that your product identifies as fraudulent
- All the Web site URLs that you visited before the detection of a risk
- The applications and processes that run on your computer regularly and during any security risk detection
- Response instances that your computer sends to any potential security risk

- General system information and performance attributes from the computer
- General information about your computer such as idle time, standby, and screensaver settings

After the potential security risks are assessed from the submitted data, Symantec sends the information back to Norton Internet Security. The Norton features such as Norton Insight and Insight Network use this information to identify files and processes at risk.

You should participate in Norton Community Watch submissions to provide valuable contribution to the entire community that uses Norton security products. Symantec maintains an adequate level of protection for the collected information. To allow or deny the detailed data submissions, you must configure the **Detailed Error Data Collection** option under **Norton Community Watch**. To access the **Detailed Error Data Collection** option, go the Norton Internet Security main window, and then click **Settings > General > Other Settings > Detailed Error Data Collection**. The detailed data may vary depending on the Norton-specific errors and components. You can configure the option to manage the data submissions.

Norton Community Watch collects and submits detailed data about the Norton-specific errors and components only. It does not collect or store any personal information of any user.

If you chose not to join Norton Community Watch when you installed your Norton product, you can turn it on later. To access the **Norton Community Watch** option, go to the Norton Internet Security main window, and then click **Settings > General > Other Settings > Norton Community Watch**. You can also review the data, which Norton Community Watch collects and submits to Symantec, in the **Security History** window.

About Norton Bootable Recovery Tool

Norton Bootable Recovery Tool scans and removes viruses, spyware, and other security risks from your computer. Your computer might be infected with a virus if you experience any of the following symptoms:

- You cannot install Norton Internet Security.
- You cannot start your computer.
- Your computer is extremely slow.

Norton Bootable Recovery Tool is integrated with Windows Preinstallation Environment (WinPE). Therefore, you can run Norton Bootable Recovery Tool only from a CD, DVD, or USB key. You must use Norton Bootable Recovery Tool Wizard to create the Norton Bootable Recovery Tool CD, DVD, or USB key.

You cannot run Norton Bootable Recovery Tool in WinPE for more than 72 hours. If you run Norton Bootable Recovery Tool for more than 72 hours, your computer restarts without any notification.

You can use the Norton Bootable Recovery Tool CD, DVD, or USB key to recover a computer that is infected with viruses and other security threats. This security program is not a replacement for continuous, real-time protection from viruses and latest security risks. To protect your computer from future infections, be sure to install or continue using Norton Internet Security that you already purchased.

Norton Bootable Recovery Tool detects and resolves the following security threats:

Viruses	Programs that infect another program, boot sector, partition sector, or document by inserting themselves or attaching themselves to that medium. Most viruses just replicate; many also do damage.

Trojan horses	Programs containing malicious codes that are disguised as or hiding in something benign, such as a game or utility.
Hacking tools	Tools that are used by a hacker to gain unauthorized access to your computer. One type of hacking tool, a keystroke logger, tracks and records your individual keystrokes and can send this information back to the hacker.
Spyware	Programs that can scan systems or monitor activity and relay the information to other computers or locations in cyberspace.
Adware	Programs that facilitate the delivery of advertising content through their own window, or by using another program's interface.

Trackware	Programs that track system activity, gather system information, or track user habits, and relay this information to third-party organizations. The information that is gathered by such programs is neither personally identifiable nor confidential. Trackware programs are installed with the user's consent, and may also be packaged as part of other software that is installed by the user.

Downloading the Norton Bootable Recovery Tool Wizard

If your attempt to install a Norton product fails, you can download the Norton Bootable Recovery Tool Wizard. This easy-to-use wizard helps you create Norton Bootable Recovery Tool on a CD, DVD, or USB key. You can use Norton Bootable Recovery Tool to scan your computer and remove any security threats that prevent successful installation.

It is recommended that you download and install Norton Bootable Recovery Tool Wizard on a computer that does not have any security threats and create Norton Bootable Recovery Tool. If you create Norton Bootable Recovery Tool on an infected computer, there is a chance that the recovery CD, DVD, or USB key might get infected.

To use Norton Bootable Recovery Tool, you must use the product key of the Norton product that you purchased. If you use a trial version of Norton Internet Security, you need to create a Norton Account to receive a product key to use Norton Bootable Recovery Tool.

You can download Norton Bootable Recovery Tool Wizard in one of the following ways:

- From the **Start** menu.
- From the Norton Support Web site.

To download the Norton Bootable Recovery Tool Wizard from the Start menu

1. On the Windows taskbar, do one of the following:
   - In Windows XP, click **Start > Programs > Norton Internet Security > Norton Recovery Tools**.
   - In Windows Vista or Windows 7, click **Start > All Programs > Norton Internet Security > Norton Recovery Tools**.
2. Follow the on-screen instructions.

To download the Norton Bootable Recovery Tool Wizard from the Internet

1. Open your Web browser, and go to the following URL:
   http://www.norton.com/recoverytool
2. Follow the on-screen instructions.

To download the Norton Bootable Recovery Tool Wizard from Norton Internet Security

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the **Computer Scan** pane, do one of the following:
   - Click **Quick Scan**.
   - Click **Full System Scan**.
3. At the bottom of the scan window, next to **If you think there are still risks**, click **click here**.
4. In the **Norton Rescue Tools** Web page, click **Download Norton Bootable Recovery Tool**.
5. Follow the on-screen instructions.

Using the Norton Bootable Recovery Tool

If the installation of your Norton product fails, you can use the Norton Bootable Recovery Tool to scan and remove any security threats that prevent successful installation. If your computer is infected and you are not able to start your Windows operating system, you can use Norton Bootable Recovery Tool to remove threats and recover your computer.

Norton Bootable Recovery Tool is available on the product CD that you purchased. You can use the product CD as a recovery media.

To use Norton Bootable Recovery Tool, you must use the product key of the Norton product that you purchased. If you use a trial version of Norton Internet Security, you need to create a Norton Account to receive a product key to use Norton Bootable Recovery Tool.

To use the Norton Bootable Recovery Tool

1. Insert the recovery media and start your computer from the recovery media.
   The recovery media can be a Norton Bootable Recovery Tool CD, DVD, USB key, or the product CD.
2. Read the **Norton License Agreement**, type your product key, and then click **I Agree**.
   If you use a non-QWERTY keyboard, use the **Virtual Keyboard** option to enter your product key.
3. In the **Norton Bootable Recovery Tool** window, click **Norton Advanced Recovery Scan**.
4. Click **Start Scan**.
5. After the scan is complete, remove the recovery media from the drive or USB port, and restart your computer.

Starting Norton Internet Security from the command prompt

If you work from the command line (for example, writing a script or code), you can start Norton Internet Security while you are still in DOS.

To start Norton Internet Security from the command prompt

1. At the command-line prompt, type the directory where Norton Internet Security is located, and the executable.
   - In 32-bit version of Windows, Norton Internet Security and the executable are located at the following path:

     \Program Files\Norton Internet Security\Engine*version*\Uistub.exe

     Where *version* represents the version number of installed Norton Internet Security.
   - In 64-bit version of Windows, Norton Internet Security and the executable are located at the following path:

     \Program Files (x86)\Norton Internet Security\Engine*version*\Uistub.exe

     Where *version* represents the version number of installed Norton Internet Security.
2. Press **Enter**.

About the Norton Internet Security icon

After you install Norton Internet Security, it displays an icon in the notification area at the far right of the Windows taskbar. This icon indicates the current status of your computer.

Norton Internet Security displays alerts and notifications to inform you how viruses and other security threats are detected and resolved. These alerts

and notifications appear over the notification area of your computer. In most cases, you can click the link available in the alert to view the details and fix the problems.

The Norton Internet Security icon represents the current state of your computer. The icon changes its color when it actively fixes any issues or wants to inform you about any warning or urgent issues.

You can see the following representations of Norton Internet Security icon in the notification area:

Icon with a green badge	Represents that your computer is completely secure
Icon with an orange badge	Represents that there are some issues against your computer protection that require your attention
Icon with a red badge	Represents that there are some urgent issues against your computer protection that require immediate resolution
Icon with a gray badge	Represents that your product is disabled
Icon with a yellow badge	Represents that Norton Internet Security is fixing issues
Icon with a crescent-pattern	Represents that the Silent Mode feature is turned on This icon also displays the current protection status badge.

You can right-click the Norton Internet Security icon to open the shortcut menu to quickly access a few important tasks of Norton Internet Security.

About Norton Internet Security shortcut menu

Norton Internet Security performs background activities to keep your computer secure. The icon in the notification area reassures you that your protection is up to date. The icon changes its color if any change in status occurs.

The messages that appear in the notification area might require a response from you, such as opening a window, and taking an action. More often, messages inform you about current activities, and they disappear after a few seconds. You can check the **Security History** window for any further details.

You can right-click the Norton Internet Security icon to access specific Norton Internet Security activities. Depending on the current activities, your options include the following:

Open Norton Internet Security	Lets you launch the Norton Internet Security main window to complete tasks, view current status, or access other features.
Run QuickScan	Lets you run a Quick Scan to protect possible virus-infected areas of your computer.
Run LiveUpdate	Lets you run LiveUpdate to check for definition and program updates.
View Recent History	Lets you review the information about the security events for all of the categories.
Get Support	Lets you resolve your problem easily using Norton Autofix.

Turn on/Turn off Silent Mode	Lets you turn on or turn off Silent Mode.
Disable/Enable Smart Firewall	Lets you turn off or turn on the firewall.
Disable/Enable Antivirus Auto-Protect	Lets you turn off or turn on Antivirus Auto-Protect.
Check for New Version	Lets you check if new version of your product is available or not. This option is available only if you have activated your product and you have an active subscription.

About LiveUpdate

Symantec products download the latest definition updates and program updates regularly from Symantec servers. The definition updates protect your computer from the latest viruses and unknown security threats. Using the LiveUpdate technology, Symantec products help you to obtain and install these updates.

LiveUpdate takes little time to download and process the definition updates and program updates. You can choose Smart Definitions to minimize download time, installation time, and memory consumption as Smart Definitions are a subset of virus definitions. To access the **Smart Definitions** option, go to the Norton Internet Security main window, and then click **Settings > Updates > Smart Definitions**. You can cancel the LiveUpdate session at any time.

LiveUpdate obtains these updates for your computer by using your Internet connection. If your network uses proxy servers to connect to the Internet, LiveUpdate uses the proxy settings in your product to

download the latest updates. To configure the proxy settings of your network, go to the Norton Internet Security main window, and then click **Settings > Network > Network Security Settings > Proxy Server > Configure**.

LiveUpdate does not download the latest definition updates and program updates, if the **Metered Broadband Mode** option in the **Settings** window is set to **No Traffic**. Metered Broadband Mode lets you define the amount of network bandwidth that Norton Internet Security can use. Therefore, you must ensure that the **Metered Broadband Mode** option is turned on and set to **No Limit** or **Critical Updates Only** for LiveUpdate to run successfully.

About Program and Definition Updates

LiveUpdate obtains program updates and definition updates for your computer by using your Internet connection.

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of the entire product. Program updates are usually created to extend the operating system or hardware compatibility, adjust a performance issue, or fix program errors. Program updates are released on an as-needed basis.

Some program updates may require that you restart your computer after you install them.

LiveUpdate automates the process of downloading and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the older files and downloaded definitions from the temporary folder after processing the updates.

Definition updates are the files that keep your Symantec products up to date with the latest antithreat technology. The definition updates that you receive depend on which product you use.

The type of definition updates that each of the Symantec products receive are as follows:

Norton AntiVirus, Norton AntiVirus Online	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats.
Norton Internet Security, Norton Internet Security Online	In addition to the virus and security risk updates, users of these products receive definition updates for security protection. For the products that contain protection against phishing, users receive definition updates against phishing. The security definition updates provide the latest predefined firewall rules, the updated lists of applications that access the Internet, Intrusion Prevention signatures, and Symantec spam definition files. These lists are used to identify unauthorized access attempts to your computer.

Norton 360, Norton 360 Online	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats. In addition, users of these products receive Symantec spam definition files and definition updates against phishing.
Norton Security Suite, Norton Business Suite	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats. In addition, users of these products receive Symantec spam definition files and definition updates against phishing.

About Smart Definitions

Norton Internet Security downloads and installs virus definitions regularly to protect your computer from the latest security threats. For faster downloads and installation purpose, Norton Internet Security classifies these virus definitions into two sets.

The virus definitions are classified into the following two sets:

Complete Set	Contains all the virus definitions for each threat that is known to Symantec.

Core Set	Contains the most important virus definitions that are required for latest security threats as viewed by Symantec. The Core Set is a subset of the Complete Set, and it is approximately 30 percent smaller than the Complete Set. The Core Set minimizes download time, installation time, and system start time. It also occupies lesser amount of disk space as compared to the Complete Set virus definitions. Therefore, the Core Set results in faster performance of your computer.

The Core Set virus definitions are called as Smart Definitions. Norton Internet Security provides the **Smart Definitions** option to choose between Core Set virus definitions and Complete Set virus definitions for LiveUpdate sessions. To access the **Smart Definitions** option, go to the Norton Internet Security main window, and then click **Settings > Updates > Smart Definitions**.

During Automatic LiveUpdate or each time that you run LiveUpdate manually, Norton Internet Security checks if the **Smart Definitions** option is turned on or off. It then downloads and installs the desired set of virus definitions based on the option settings. By default, the **Smart Definitions** option is turned on, which means that the Core Set virus definitions are downloaded and installed.

Turning off or turning on Smart Definitions

Smart Definitions are a subset of virus definitions that contains most important definitions for the latest security threats.

As the Smart Definitions are of considerably smaller size, it results in lesser download time, lesser installation time, lesser boot time, and lesser memory consumption. It also occupies lesser amount of disk space as compared to the full set of virus definitions. Therefore, Smart Definitions result in faster performance of your computer.

Norton Internet Security checks the **Smart Definitions** option settings during each LiveUpdate session. If the option is turned on, the Smart Definitions are downloaded and installed. If the option is turned off, all of the virus definitions are downloaded and installed.

To turn off or turn on Smart Definitions

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Updates**.
3. In the **Smart Definitions** row, do one of the following:
   - To turn off Smart Definitions, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Smart Definitions, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **OK**.

About running LiveUpdate

You should run LiveUpdate as soon as you install Norton Internet Security. Some Symantec products run LiveUpdate automatically to keep your protection up to date. If you do not use the **Automatic LiveUpdate** option, you should manually run LiveUpdate once a week.

In addition to the definition updates that Automatic LiveUpdate downloads, the product uses streaming technology to download the latest virus definitions.

These downloads are called Pulse Updates. The Pulse Updates are lighter and faster than Automatic LiveUpdate. It keeps your computer secure from the ongoing threats on the World Wide Web.

When Pulse Updates are enabled, LiveUpdate checks for definition updates every few minutes and downloads the streamed virus definitions. The Pulse Updates protect your computer from the latest security threats without compromising your system performance. Even if you turn off Pulse Updates, LiveUpdate picks all the missed streams and it updates your computer during the full definition updates.

Each LiveUpdate session checks if the **Smart Definitions** option is turned on or off, and downloads and installs the updates based on the option settings. To access the **Smart Definitions** option, go to the Norton Internet Security main window, and then click **Settings > Updates > Smart Definitions**. By default, the **Smart Definitions** option is turned on. As Smart Definitions are only a subset of all the virus definitions, you can minimize download time, installation time, and memory consumption. However, if you want all of the virus definitions to be downloaded and installed, you can turn off the **Smart Definitions** option.

Checking for updates manually

LiveUpdate checks for updates to the product that is installed on your computer.

These updates protect your computer from newly discovered threats. LiveUpdate uses the Internet connection to connect to the Symantec server, checks for updates, and then downloads and installs them automatically.

You should have the **Automatic LiveUpdate** option turned on to ensure that you have the latest definition updates and program updates. Definition updates contain the information that allows the product to recognize and alert you to the presence of a specific virus or security threat. Symantec issues program

updates periodically, which are enhancements to the product. Program updates are usually created to fix program errors, improve the performance of the program, or, to extend the operating system or hardware compatibility. After you install program updates, you might not necessarily see a difference in the way that the product works.

If you are not connected to the Internet, connect to the Internet first, and then run LiveUpdate. Or, if you use a proxy server to connect to the Internet, configure the proxy settings, and then run LiveUpdate. To configure the proxy settings of your network, go to the Norton Internet Security main window, and then click **Settings > Network > Network Security Settings > Proxy Server > Configure**.

When the LiveUpdate session is complete, you can use the **View Summary** link to view the summary of the updates that are installed on your computer.

To check for updates manually

1. In the Norton Internet Security main window, click **LiveUpdate**.
   LiveUpdate connects to the Symantec server, checks for available updates, and then downloads and installs them automatically.
2. In the **Norton LiveUpdate** window, when the installation is complete, click **OK**.
   Some program updates may require you to restart your computer after you install them.

About keeping your protection up to date

Definition updates are available to you as long as you maintain an active product status. The ways in which

you can acquire the product and maintain your status are as follows:

If you purchased a subscription version of a retail product	The product includes a limited-time subscription to definition updates. When the subscription is due to expire, you are prompted to renew. Follow the on-screen instructions to complete your subscription renewal. After your product expires, you cannot obtain updates of any kind and all the security features are turned off. If you do not renew your product, you are no longer protected against security threats. Though LiveUpdate continues to check for updates after expiration, you must renew your product to enable all the security features.
If you purchased a product as a service, or it came installed on your computer	If you do not activate your service or renew your subscription, you cannot obtain updates of any kind and the software no longer functions.
If you receive this service through your service provider	Your product status is always active as long as your security service is active with your service provider. If your security service is not active, you cannot obtain updates of any kind and the software no longer functions.

Turning off or turning on Automatic LiveUpdate

You can have LiveUpdate check for definition updates and product updates automatically on a set schedule, by turning on the **Automatic LiveUpdate** option. You can also run LiveUpdate manually when the **Automatic LiveUpdate** option is turned on. However, you must

run LiveUpdate manually to obtain updates if you have turned off the **Automatic LiveUpdate** option.

If you are connected to the Internet, Automatic LiveUpdate downloads product updates and definition updates every hour. If you have an Integrated Services Digital Network (ISDN) router that is set to automatically connect to your Internet service provider (ISP), it may incur charges each time. If you do not want this setup, you can turn off the automatic connection on your ISDN router, or turn off the **Automatic LiveUpdate** option.

To turn off Automatic LiveUpdate

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Updates**.
3. In the **Automatic LiveUpdate** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.
5. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Automatic LiveUpdate, and then click **OK**.
6. In the **Settings** window, click **OK**.

To turn on Automatic LiveUpdate

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Updates**.
3. In the **Automatic LiveUpdate** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, Click **Apply**.
5. Click **OK**.

About Pulse Updates

In addition to the definition updates that Automatic LiveUpdate downloads, Norton Internet Security uses streaming technology to download the latest virus definitions. These downloads are called Pulse Updates. The Pulse Updates are lighter and faster than Automatic LiveUpdate. They keep your computer secure from the ongoing threats that exist on the Internet. Pulse Updates protect you against the rapidly-changing environment of security threats without compromising your computer's performance. Pulse Updates should always be turned on to get the latest updates.

Pulse Updates checks for definition updates every 5 minutes. If definition updates are available, LiveUpdate downloads the streamed virus definitions. Pulse Updates provide the updates in between the full updates, which Automatic LiveUpdate downloads automatically every hour. Norton Internet Security merges the new stream that is downloaded with the last updates that are installed. The Pulse Updates downloads provide additional and fast protection for the latest threats in between the full updates without disrupting your online experience.

Even if you do not turn on Pulse Updates, LiveUpdate collects all the missed streams and, it updates your computer during full definition updates.

Turning off or turning on Pulse Updates

Pulse Updates provide frequent, lightweight updates every 5 minutes in between the full updates. Always ensure that the **Pulse Updates** option is turned on. It protects you from the latest threats without compromising your system performance or disrupting your online experience.

You must be connected to the Internet to obtain latest definition updates by using Pulse Updates. You can

turn on or turn off **Pulse Updates** only if **Automatic LiveUpdate** is turned on.

To turn off or turn on Pulse Updates

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Updates**.
3. Under **Automatic LiveUpdate**, in the **Pulse Updates** row, do one of the following:
   - To turn off Pulse Updates, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Pulse Updates, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **OK**.

About Network Proxy settings

A proxy server regulates access to the Internet, and prevents external computers from accessing your network. If you are on a network that uses a proxy server to connect to the Internet, you can provide proxy server details to Norton Internet Security. You can use the **Network Proxy Settings** window to specify the automatic configuration URL, the proxy settings, and the authentication details. Norton Internet Security uses the proxy settings and authentication details to connect to the Internet automatically, whenever required. For example, LiveUpdate uses the specified proxy server settings to retrieve updates. You must ensure that you specify the proxy server details for LiveUpdate to run successfully.

In some cases, your network uses an automatic configuration URL or script for managing Internet access. In this case, you must provide the URL of the required Proxy Automatic Configuration (PAC) file. A PAC file contains the code that lets your browser know about the proxy settings for different Web sites over

the Internet. It also contains the words which you want to filter and block while you access the Internet. You can also choose the option that lets your browser to automatically detect the proxy settings. If you want your manual settings in the network, ensure that you disable the **Automatic Configuration** options.

Network Proxy Settings window lets you specify the following settings:

Automatic Configuration	Lets you specify the automatic configuration URL or script to manage Internet access. You have the following options: ▪ **Automatically detect settings** Lets your browser detect the network settings automatically. If you do not want to override your manual settings for network connections, you must disable this option. ▪ **Use automatic configuration script** Lets your browser use the automatic configuration URL or script to manage Internet access. Use the **URL** box to provide the HTTP URL or the script to the required PAC file (such as file://C:/Proxy.pac).

Proxy Settings	Lets you provide the details of your Proxy Settings. Under **Proxy Settings**, check **Use a proxy server for your HTTP connections**, and do the following: ▪ In the **Address** box, type the URL or IP address of your proxy server. ▪ In the **Port** box, type the port number of your proxy server. You can specify a value from 1 to 65535.
Authentication	Lets you connect to the Internet through a server that requires authentication. Use the **Username** box and **Password** box to type the authentication details.

Configuring Network Proxy Settings

When you use a proxy server to connect to the Internet, you must specify the proxy server details. The **Network Proxy Settings** window lets you enter automatic configuration settings, proxy settings, and proxy server authentication settings. The Network Proxy settings let you connect to the Internet while you perform tasks such as activating the product or accessing the support options.

To configure Network Proxy Settings

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Network Security Settings**.
4. In the **Proxy Server** row, click **Configure**.

5 In the **Network Proxy Settings** window, do the following:

- If you want your browser to automatically detect network connection settings, under **Automatic Configuration**, check **Automatically detect settings**.
- If the proxy server requires an automatic configuration URL, under **Automatic Configuration**, check **Use automatic configuration script**. Type the URL (such as file://C:/Proxy.pac) in the **URL** box.
- If your network uses a proxy server, under **Proxy Settings**, check **Use a proxy server for your HTTP connections**. In the **Address** box, type the URL or IP address of your proxy server, and in the **Port** box, type the port number of your proxy server. You can specify a value from 1 to 65535.
- If your proxy server requires a user name and password, under **Authentication**, check **I need authorization to connect through my firewall or proxy server**. Type the user name in the **Username** box and password in the **Password** box.

6 In the **Network Proxy Settings** window, click **Apply**.

Monitoring your system's performance

2

This chapter includes the following topics:

- About System Insight

About System Insight

Norton Internet Security continuously monitors your computer to keep it free of any problems and run at peak efficiency. Norton Internet Security constantly scans the vital areas of your computer including memory, registry keys, and running processes. It monitors the important activities such as general file operation, network traffic, and Internet browsing. In addition, Norton Internet Security ensures that the activities that it performs on your computer do not degrade the overall performance of your computer.

System Insight provides you a centralized location where you can view and monitor the activities that you perform on your system. System Insight displays such information in the **Performance** window.

You can use the **Performance** window for the following:

- To view monthly history of the important system activities that you performed or that occurred over a period of the last three months

  The Events graph that appears at the top of the window provides a pictorial representation of important system activities. The activities include application installations, application downloads,

disk optimizations, threat detections, performance alerts, or Quick Scans. The graph displays the activities as icon or stripe, and the description for each icon or stripe is provided at the bottom of the graph. The pop-up that appears when you move the mouse pointer over an icon provides you the details about the activity. The **View Details** link in the pop-up lets you view additional details about the activity in the **Security History** window. You can use the tabs at the top of the graph to obtain details for the current month and details for the last two months.

- To rearrange the organization of files on your system

  Optimizing your system helps you maximize the usable free space on a disk by grouping files based on how they are accessed. The **Optimize** option at the top of the Events graph lets you defragment your system.

- To view and analyze the effect of Norton Internet Security on the performance of your computer

  The Performance graph that appears at the bottom of the window provides a graphical representation of your CPU usage and memory usage. The **CPU** tab displays a graph that represents the overall system CPU usage and Norton-specific CPU usage. When you click at any point on the CPU graph and memory graph, Norton Internet Security displays a list of the processes that consume maximum resources at that point. It also displays the percentage of usage for each process. You can click a process that is available in the list to get more information about the process in the **File Insight** window. The **Memory** tab displays a graph that represents overall memory usage and Norton-specific memory usage. You can select any of the **Zoom** options to obtain magnified view or historical data of the graphs.

- To view the details of Norton-specific jobs that are currently running in the background

The **Norton Tasks** window provides the details such as the timestamp, the duration, and the status of the background jobs. The details also include the type of power the job needs to run and if a job ran during idle time. You can select different power sources for the background jobs. You can also start or stop a background job at any time.

- To view the details of the Files of Interest

  The **Norton Insight - Application Ratings** window provides details on the trust level, prevalence, resource usage and stability ratings for the Files of Interest.

You can use the **Performance Monitoring** option to monitor the performance of your computer. To access the **Performance Monitoring** option, go to the Norton Internet Security main window, click **Settings > General > Performance Monitoring > Performance Monitoring** .

You can also use the **Learn More** link in the **Performance** window to access the online tutorial page to get more information.

Accessing the Performance window

System Insight provides you a centralized location where you can view and monitor your system activities. System Insight displays such information in the **Performance** window. You can access the **Performance** window to view details about the important system activities, CPU usage and memory usage, and Norton-specific background jobs. You can also view Norton Insight details and defragment your boot volume.

To access the Performance window

- In the Norton Internet Security main window, click **Performance**.

About monitoring system activities

System Insight provides information about the important system activities that you performed or that occurred over a period of the last three months. System Insight displays the information in the **Performance** window. The Events graph at the top of the **Performance** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. You can use the tabs at the top of the graph to obtain details for the current month and for the last two months. The activities include:

Installs	Provides the details about the installation activities that you performed on your system over a period of the last three months The details include the application that you installed, the date on which you installed the application, and the total number of installations on that date.
Downloads	Provides the details about the application-download activities that you performed on your system over a period of the last three months The details include the date on which you downloaded a file and the total number of downloads on that date. You can click the file name link to view additional details about the downloaded file such as the Download Insight report, file name, reputation level, and recommended action.

Optimized	Indicates the optimization activities that you performed on your system over a period of the last three months
Detections	Provides the details about the threat detection activities that Norton Internet Security performed on your system over a period of the last three months The details include the date on which Norton Internet Security detected a threat and the total number of threats that Norton Internet Security detected on that date. The **View Details** link provides additional details about the risk such as the risk impact and the origin of the risk. The details also include the action that a threat has performed on your system and the action that Symantec recommends you to resolve the threat.
Alerts	Provides the details about the performance alerts that Norton Internet Security displayed over a period of the last three months The details include the monitored date and the number of performance alerts generated. The **View Details** link provides additional details about performance-related activities, program name, program location, and system resources utilization.

Quick Scans	Provides the details about Quick Scans that Norton Internet Security performed on your system over a period of the last three months The details include the date on which a Quick Scan was performed and the number of Quick Scans that were performed on that date. The **View Details** link provides additional details such as the scan time, total items scanned, total risk detected, total risks resolved, and recommended action.

Viewing details of your system activities

System Insight lets you view details of the system activities that you performed or that occurred over the last three months in the **Performance** window. The activities include application installations, application downloads, disk optimizations, threat detections, performance alerts, or Quick Scans. You can use the tabs at the top of the Events graph to obtain details for the current month and for the last two months. The Events graph at the top of the **Performance** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. The pop-up that appears when you move the mouse pointer over an icon provides you the details about the activity. The details include the date on which an activity was performed and the number of such activities that you performed on that date. The **View Details** link provides additional details of the activity in the **Security History** window.

To view details of your system activities

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, at the top of the Events graph, click the tab for a month to view the details.
3. In the Events graph, move the mouse pointer over the icon or the stripe for an activity.
4. In the pop-up that appears, view the details of the activity.
5. If the **View Details** option appears in the pop-up, click **View Details** to view additional details in the **Security History** window.

About performance alerting

Norton Internet Security monitors your system performance. If it detects an increased usage of system resources by any program or process, it notifies you with performance alerts. Performance alerting works only when the **Performance Monitoring** option and **Performance Alerting** option are turned on.

Performance alerting notifies you with information about the program name and resources that the program uses excessively. The **Details & Settings** link in the performance notification alert lets you view additional details about the resource consumption by the program. The **File Insight** window opens and displays the details of the file, the origin of the file, and the complete resource usage list of the program. From the **File Insight** window, you can choose to exclude the program from being monitored. You can use the **Settings** option in the **File Insight** window to turn off the **Performance Alerting** option.

Performance alerts are not displayed when your computer is idle or in Silent Mode.

For each system resource, such as CPU, memory, and hard disk, there is a resource consumption threshold defined. When the resource consumption of a program

exceeds the defined threshold limit, Norton Internet Security alerts you with a performance alert.

You can use the **Resource Threshold Profile for Alerting** option to configure the threshold limit. To access the **Resource Threshold Profile for Alerting** option, go to the Norton Internet Security main window, and then click **Settings > General > Performance Monitoring > Resource Threshold Profile for Alerting**.

You can use the **Use Low Resource Profile On Battery Power** option to let Norton Internet Security automatically change the resource threshold profile to low when your computer runs on battery power.

In addition, you can add programs to the **Program Exclusions** list using the **Program Exclusions** option. When you add a program to the **Program Exclusions** list, Norton Internet Security does not alert you when the program exceeds the resource consumption threshold limit.

You can view all the performance-related logs under the **Performance Alert** category in the **Security History** window.

Configuring performance alerts

You can use the **Performance Alerting** option to receive performance alerts when there is an increased usage of system resources by any program or process.

You can use the following options to configure performance alerts:

Off	Turns off performance alerts. Select this option if you do not want Norton Internet Security to notify you with performance alerts.

On	Turns on performance alerts. Select this option if you want Norton Internet Security to notify you with performance alerts when a program or process exceeds the system resource usage threshold limit. By default, the **Performance Alerting** option is turned on.
Log Only	Monitors and records the system resource usage. Select this option if you want Norton Internet Security to only monitor the system resource usage of every program or process running on your computer. When a program or process exceeds the system resource usage threshold limit, Norton Internet Security records these details in the **Security History** window. You can view the details that are related to performance alerts under **Performance Alert** category in the **Security History** window.

To configure performance alerts

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Performance Monitoring**.

4 Under **Performance Monitoring**, in the **Performance Alerting** row, do one of the following:
   - To turn off performance alerts, move the **Performance Alerting** switch to the **Off** position.
   - To turn on performance alerts, move the **Performance Alerting** switch to the **On** position.
   - To suppress the performance alerts, move the **Performance Alerting** switch to the **Log Only** position.
5 Under **Alert for High Usage of**, do the following:
   - If you want Norton Internet Security to monitor the CPU usage, move the **CPU** switch to the **On** position. By default, this switch is turned on.
   - If you want Norton Internet Security to monitor the memory usage, move the **Memory** switch to the **On** position. By default, this switch is turned on.
   - If you want Norton Internet Security to monitor the disk usage, move the **Disk** switch to the **On** position. By default, this switch is turned on.
   - If you want Norton Internet Security to monitor the handle count, move the **Handles** switch to the **On** position.
6 Click **Apply**, and then click **OK**.

Configuring the resource threshold profile

The threshold limit for the system resources determines at which point Norton Internet Security should notify you with performance alerts. When a specific program exceeds the threshold limit of using your system resource, Norton Internet Security notifies you with a performance alert.

To configure the resource threshold profile

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **General** tab.
3 In the left pane, click **Performance Monitoring**.

4 Under **Performance Monitoring**, in the **Resource Threshold Profile for Alerting** row, select one of the following options:

Low	Configures a low threshold limit for alerting If you choose this option, Norton Internet Security notifies you with performance alerts whenever a program reaches the lowest threshold limit of using your system resource. Symantec recommends you to select this option when your computer runs on battery power.
Medium	Configures a medium threshold limit for alerting By default, the threshold limit is set to medium.
High	Configures a high threshold limit for alerting. If you choose this option, Norton Internet Security notifies you with performance alerts whenever a program reaches the highest threshold limit of using your system resource.

5 Click **Apply**, and then click **OK**.

Turning off or turning on the Use Low Resource Profile On Battery Power option

When your computer runs on battery power, it is important that all active software programs consume minimum resource usage. By reducing resource usage, your computer gains longer battery life and becomes more energy efficient.

You can configure a low threshold profile and ensure that all programs consume minimum resource usage. When the resource usage of a program or a process exceeds the low threshold limit, Norton Internet Security notifies you with a performance alert. You can choose to close the program or the process manually and free the resource.

If the **Use Low Resource Profile On Battery Power** option is turned on, Norton Internet Security automatically changes the threshold profile to low when your computer runs on battery power. By default, this option is turned on.

Symantec recommends that you keep the **Use Low Resource Profile On Battery Power** option turned on.

To turn off the Use Low Resource Profile On Battery Power option

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Performance Monitoring**.
4. Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **Apply**, and then click **OK**.

To turn on the Use Low Resource Profile On Battery Power option

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.

3 In the left pane, click **Performance Monitoring**.
4 Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to the left to the **On** position.
5 Click **Apply**, and then click **OK**.

Excluding programs from appearing in performance alerts

Norton Internet Security lets you exclude programs from appearing in performance alerts. You can add the programs that consume high CPU, memory, or disk usage to the **Program Exclusions** list. When you add a program to the **Program Exclusions** list, Norton Internet Security does not alert you when the program exceeds the resource consumption threshold limit.

To exclude a program from appearing in performance alerts

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **General** tab.
3 In the left pane, click **Performance Monitoring**.
4 Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
5 In the **Program Exclusions** window, click **Add**.
6 In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
7 Click **Open**.
8 In the **Program Exclusions** window, click **OK**.
9 In the **Settings** window, click **Apply**.
10 Click **OK**.

Removing programs from Program Exclusions

The **Program Exclusions** window lists all the programs that are excluded from appearing in performance alerts. If you want, you can remove any of the programs that you already added to the **Program Exclusions**

window. When you remove a program, the program appears in the performance alert the next time it crosses the resource consumption threshold limit.

To remove a program

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Performance Monitoring**.
4. Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
5. In the **Program Exclusions** window, select the program that you want to delete, and then click **Remove**.
6. Click **OK**.
7. In the **Settings** window, click **Apply**.
8. Click **OK**.

About CPU graph and memory graph

Norton Internet Security monitors the overall system CPU usage and memory usage and the Norton-specific CPU usage and memory usage. Norton Internet Security displays the details in the CPU graph and the memory graph. The CPU graph and memory graph are real-time graphs of CPU utilization and memory utilization.

The graphs display a performance time for the last 90 minutes or for the duration since you started your computer. The graphs update the information at an interval of every 15 seconds. The graphs progress from right to left, and the most recent data appear on the far right of the graph. The blue pattern in the graphs depicts the overall system usage, and the yellow pattern depicts the Norton-specific usage. The gray blocks that are labeled as **Idle** indicate the idle period of your computer. The gray blocks include the period when your computer is in shutdown, sleep, or log out state.

The graphs show a default performance time of 90 minutes. However, you can use the **Zoom** options to

define a region of the graph that you are interested to view. You can select a **Zoom** option to obtain magnified view or historical data of the graphs. For example, if you select the **10min** option, Norton Internet Security displays the magnified view of CPU graph or memory graph for the last 10 minutes. If you select the **1d** option, Norton Internet Security displays a historical data of the last one day.

When you click at any point on the CPU graph or memory graph, Norton Internet Security displays a list of the processes that consume maximum resources at that point. It also displays the percentage of usage for each process. You can click a process that is available in the list to get more information in the **File Insight** window.

The **File Insight** window provides information about the process such as:

- The file name, version number, digital signature, the date on which the process was installed
- The date on which the process was last used and whether it is a startup file
- The stability details
- The confidence level
- The resource usage details
- The actions that the process performs on your system

In addition, the **File Insight** window displays the CPU graph and the resource usage details for the running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage by the process.

Viewing the CPU graph and memory graph

Norton Internet Security monitors the overall system CPU usage and memory usage and the Norton-specific CPU usage and memory usage. The **CPU** tab and the **Memory** tab at the top of the Performance graph display the CPU graph and the memory graph respectively.

The **Zoom** options provide you the magnified view of the CPU graph and memory graph. For example, if you select the **10min** option, Norton Internet Security displays the magnified view of CPU graph or memory graph for the last 10 minutes. If you select the **30min** option, Norton Internet Security displays a magnified view of the CPU graph and memory graph for the last 30 minutes.

By default, the graphs display performance time for the last 90 minutes.

To view CPU graph and memory graph

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
   - To obtain a magnified view, click **10min** or **30min** next to the **Zoom** option

Obtaining historical data of your CPU and memory usage

The **Zoom** options also provide you the historical data of the CPU graph and memory graph. For example, if you select the **1d** option, Norton Internet Security displays the data of CPU graph or memory graph for the last one day.

To view historical data of your CPU or memory usage

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.

3 Do one of the following:
- To obtain historical data for the last one day, click **1d**.
- To obtain historical data for the last one week, click **1w**.
- To obtain historical data for the last one month, click **1m**.

Identifying resource-consuming processes

You can click at any point on the CPU graph or memory graph to obtain a list of the processes that consume maximum resources of your computer at that point. You can click a process that is available in the list to get more information about the process in the **File Insight** window.

To identify resource-consuming processes

1 In the Norton Internet Security main window, click **Performance**.
2 In the **Performance** window, do one of the following:
- To view the CPU graph, click the **CPU** tab.
- To view the memory graph, click the **Memory** tab.

3 Click at any point on the graph to obtain a list of resource-consuming processes.
4 Click the name of a process to obtain additional information about the process in the **File Insight** window.

About Startup Manager

Some programs are configured to launch during startup of your computer. The number of startup items increases as you install new applications, and the time that is required to start your computer increases as a result. Startup Manager helps to manage the startup items on your computer. For any startup program that the Startup Manager lists, you can view the detailed

information such as Community Usage and Resource Usage. You can also click the application name and view the File Insight details. These details would help you determine whether or not to enable an application during startup.

Norton Internet Security displays the community usage details under the following conditions:

- The **Norton Community Watch** option in the **Settings** window must be turned on.
- The **Metered Broadband Mode** option in the **Settings** window must be configured to **No Limit** or **Critical Updates Only**.

Startup Manager lets you view the list of programs that are included to the startup items. Based on your priority, you can configure Startup Manager to run or not run these programs when your computer starts. You can also choose to delay the start of the programs and run them manually from the Startup Manager. This way, you can enhance the performance of your computer. You can disable a program and measure the performance of your computer the next time you start your computer.

If you choose to install the latest version of Norton Internet Security, you can still retain the Startup Manager setting. When you uninstall Norton Internet Security, the programs that you had added to the Startup Manager are reset to their default startup setting.

To add a startup item, you can open your Startup folder that is available in your Windows **Start** menu and add programs as required. For more information on adding programs in Windows Startup, go to Microsoft Technical Support Web site or Windows online Help.

Disabling or enabling startup items

Whenever you start your computer, there are some programs that automatically start and run in parallel.

These programs are called startup items. The startup items increase the start time of your computer.

Startup Manager helps you manage the startup items of your computer efficiently. If you do not want a program to automatically start when you turn on your computer, you can disable the program using Startup Manager. You can also delay a startup item that you want to start at a later time.

To disable startup items

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Startup Manager**.
3. In the **Startup Manager** window, in the **On/Off** column, uncheck the program that you do not want to automatically start when you turn on your computer.
4. Click **Apply**.
5. Click **Close**.

To enable startup items

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Startup Manager**.
3. In the **Startup Manager** window, in the **On/Off** column, select the program that you want to automatically start when you turn on your computer.
4. Click **Apply**.
5. Click **Close**.

Managing startup items

Norton Internet Security Startup Manager monitors and lists the programs that automatically start when you turn on your computer. To reduce the start time of your computer and improve the performance, you can delay the start of some of the programs when you turn on your computer.

To delay startup items

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Startup Manager**.
3. In the **Startup Manager** window, in the **Delay Start** column, select the program that you want to delay.
4. Click **Apply**.
5. Click **Close**.

To run delayed startup items manually

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Startup Manager**.
3. In the **Startup Manager** window, click **Run Delayed Items Now**.
4. Wait for the program to start, and then in the **Startup Manager** window, click **Close**.

About optimization

The data storage space on a disk is divided into discrete units. These units are called clusters. When files are written to the disk, they are broken up into cluster-sized pieces. When all of the file pieces are located in adjacent or contiguous clusters, the file can be accessed quickly.

Your computer's hard disk stores all of your files, applications, and the Windows operating system. The bits of information that make up your files gradually spread over the disk. This process is known as fragmentation. The more that you use your computer, the more fragmented the hard disk gets.

When a fragmented file is accessed, the disk performance is slower. The performance is slower because the drive head locates, loads, saves, and keeps track of all of the fragments of the file. If free space is also fragmented, the drive head might have to track adequate free space to store temporary files or newly added files.

Optimization rearranges file fragments into adjacent or contiguous clusters. When the drive head accesses all of the file data in one location, the file is read into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. Optimization consolidates free space to avoid fragmenting newly added files. It adds extra space after major data structures so that they can grow without immediately becoming fragmented again.

You can optimize your boot volume manually by using the **Optimize** option in the **Performance** window.

You can also configure Norton Internet Security to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Norton Internet Security automatically schedules the optimization when it detects the installation of an application on your computer. The optimization process starts next time when your computer is idle.

You can use the **Idle Time Optimizer** option to optimize the boot volume during the idle time. To access the **Idle Time Optimizer** option, go to the Norton Internet Security main window, and then click **Settings > General > Norton Tasks > Idle Time Optimizer**.

Optimizing your boot volume

The **Optimize** option lets you optimize your boot volume to improve the boot time of your computer. Optimization of your boot volume maximizes the usable free space by rearranging file fragments into adjacent and contiguous clusters. When the drive head of your hard disk accesses all of the file data in one location, the file is read into the memory faster.

When you use the **Optimize** option in Windows XP, Norton Internet Security optimizes only the boot volume (for example, C:\Windows). Therefore, it requires less time to complete optimization. However, when you use the **Optimize** option in Windows Vista or Windows 7, Norton Internet Security optimizes the

drive that contains the boot volume. Therefore, it requires more time to complete optimization.

You can access the **Optimize** option at the top of the security status graph in the **Performance** window. You can also optimize your boot volume using the **Insight Optimizer** option in the **Norton Tasks** window. The **Insight Optimizer** row in the background jobs list that is available in the **Norton Tasks** window displays the details of the boot volume optimization process. You can view details such as timestamp, duration, and status of the background job.

To optimize your boot volume from the Performance window

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, at the top of the security status graph, click **Optimize**.

To optimize your boot volume from the Norton Tasks window

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.
3. In the **Norton Tasks** window, under the **Norton Tasks** column, click the **Play** icon that appears before **Insight Optimizer**.

About the Idle Time Optimizer

Idle Time Optimizer lets you configure Norton Internet Security to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Norton Internet Security automatically schedules the optimization when it detects the installation of an application on your computer and your computer is idle. If you start using your computer again, Norton Internet Security stops the optimization task, and starts optimizing the next time that your computer is idle. This way, the background job of

optimization does not affect the performance of your computer.

Optimization rearranges file fragments into adjacent or contiguous clusters in the hard disk. It improves the computer performance by reading the files into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. In addition, it consolidates free space to avoid fragmenting newly added files.

You can use the **Idle Time Optimizer** option to optimize the boot volume during the idle time. To access the **Idle Time Optimizer** option, go to the Norton Internet Security main window, and then click **Settings > General > Norton Tasks > Idle Time Optimizer**.

Turning off or turning on Idle Time Optimizer

Norton Internet Security automatically schedules the optimization when it detects the installation of a new application on your computer. Norton Internet Security runs this optimization only when your computer is idle.

You can use the **Idle Time Optimizer** option to optimize the boot volume during idle time. By default, this option is turned on.

To turn off Idle Time Optimizer

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Norton Tasks**.
4. In the **Idle Time Optimizer** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **Apply**, and then click **OK**.

To turn on Idle Time Optimizer

1. In the Norton Internet Security main window, click **Settings**.

2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Norton Tasks**.
4. In the **Idle Time Optimizer** row, move the **On/Off** switch to the left to the **On** position.
5. Click **Apply**, and then click **OK**.

About the Norton Tasks

The **Norton Tasks** window provides an interface where you can view and monitor all Norton-specific background tasks. Norton Internet Security runs most of the background tasks when your computer is idle. The **Norton Tasks** window provides the details of the background tasks that Norton Internet Security performs.

The details include things such as:

- The name of the Norton task

  You can use the icon that appears before the name of a background job to start or stop a background task. You can start or stop a background task at any time.
- The timestamp of the Norton task

  You can view details such as the date on which the background job last ran and the time. These details help you decide whether to start a background task or wait for Norton Internet Security to run the job during idle time.
- The duration of the Norton task

  You can view the length of time that a Norton task ran the last time. The details also help you determine the length of time a background task takes to complete if you start it.
- The background task has run during idle time or not

  This detail helps you determine if a task has already run during idle time or you should run it.
- The status of the Norton task

You can view details about the completion of the task.

- The power source that the Norton Task uses.

  You can specify the type of power source that each of the Norton Tasks uses. Use the **Configure** link that is available next to the power source icon to configure the power source for the Norton Tasks.

In addition to viewing and monitoring the background task details, you can specify the **Idle Time Out** duration. After the **Idle Time Out** duration is reached, Norton Internet Security identifies the computer as idle and run the background tasks. You can use the **Idle Countdown** bar to confirm the idle state of your computer.

You can also manually turn on Silent Mode for a specified duration.

Monitoring background jobs of Norton Internet Security

The **Norton Tasks** window provides the details of the background tasks that Norton Internet Security performs and lets you view and monitor the background tasks. Norton Internet Security runs most of the background tasks when your computer is idle. Performing all background tasks when your computer is idle helps your computer to run at peak efficiency when you use your computer. However, you can manually start or stop a task at any time. You can also specify the **Idle Time Out** duration. After the **Idle Time Out** duration is reached, Norton Internet Security identifies the computer as idle and run the background tasks. You can use the **Idle Countdown** bar to confirm the idle state of your computer. You can also view the CPU graph and memory graph to obtain the performance data of your computer.

To monitor background jobs

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.

3. In the **Norton Tasks** window, view the details of background jobs.
4. Do one of the following:
   - To run a background job, click the **Play** icon that appears before the name of the background job.
   - To stop a running background job, click the **Stop** icon that appears before the name of the background job.
5. Click **Close**.

About Power Source

You can choose the power source for Norton Internet Security to perform the Norton Tasks when the computer is idle. Norton Tasks are background tasks that Norton Internet Security performs when your computer is idle. Norton Tasks include Quick Scan, Automatic LiveUpdate, Norton Community Watch, Norton Insight, Full System Scan, Insight Optimizer, and Pulse Updates. Norton Internet Security consumes more power when it runs Norton Tasks.

By default, Norton Internet Security performs these tasks only when your computer is connected to the external power. For example, if you are in an airport, and your computer is running on battery power, Norton Internet Security does not perform the Norton Tasks. In this way, you can extend the battery power of your computer. However, you can choose the power source for Norton Internet Security to perform the Norton Tasks.

You can select one of the following options:

External	Allows the Norton Tasks to run only when your computer uses external power. If you choose this option, Norton Internet Security performs the Norton Tasks when the computer is idle and connected to external power.
External and Battery	Allows the Norton Tasks to run irrespective if the computer uses external power or battery power. If you choose this option, Norton Internet Security performs the Norton Tasks when the computer is idle. It does not consider the type of power source the computer uses.

You can configure the power source for each of the Norton Tasks.

Configuring the Power Source

You can choose the power source for Norton Internet Security to perform the Norton Tasks when the computer is idle. Norton Tasks are background tasks that Norton Internet Security performs when your computer is idle.

By default, Norton Internet Security performs these tasks only when your computer is connected to the external power. You can configure the power source for each of the Norton Tasks.

To configure the power source

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, in the left pane, click **Norton Tasks**.
3. In the **Norton Tasks** window, under the **Power Source** column, click the **Configure** link for the Norton Task that you want to configure the power source.
4. In the **Power Source** window, select one of the following:
   - **External**

     Allows the Norton Task to run only when your computer uses external power.
   - **External and Battery**

     Allows the Norton Task to run irrespective if the computer uses external power or battery power.

     If you choose this option, Norton Internet Security performs the Norton Task when the computer is idle. It does not consider the type of power source the computer uses.
5. Click **OK**.
6. In the **Norton Tasks** window, click **Close**.

About Norton Insight

Norton Insight allows the smart scanning of files on your computer. It improves the performance of Norton Internet Security scans by letting you scan fewer files without compromising the security of your computer.

A Norton Internet Security scan can identify threats on your computer in the following ways:

The Blacklist technique	At regular intervals, Norton Internet Security obtains definition updates from Symantec. These updates contain signatures of known threats. Each time when Norton Internet Security obtains the definition updates, it performs a scan of all of the files that are available on your computer. It compares the signature of the files against the known threat signatures to identify threats on your computer.

The Whitelist technique	Norton Internet Security obtains specific information about the Files of Interest and submits the information to Symantec during idle time. The information includes things such as file name, file size, and hash key. Symantec analyzes the information of each File of Interest and its unique hash value and provides a confidence level to the file. The Symantec server stores the hash value and confidence level details of the Files of Interest. The server provides the details immediately after you open the **Norton Insight - Application Ratings** window. Even the slightest modification of the file causes a change in the hash value and the confidence level of the file. Typically, most Files of Interest belong to the operating system or known applications, and they never change. These files do not require repeated scanning or monitoring. For example, Excel.exe is a file that never changes but you always scan it during a normal security scan.

Symantec assigns the following confidence levels to Files of Interest:

Good	Symantec analyzes the file as good based on the statistical evaluation that is done on the files that are available within the Norton Community. Symantec rates the trusted files as follows: ▪ If the file has three green bars, Symantec rates the file as **Norton Trusted**. The files that have three green bars display a Norton Trusted pop-up text when you move the mouse pointer over the green bars. ▪ If the file has two green bars, Symantec rates the file as **Good**. ▪ If the file has one green bar, Symantec rates the file as **Favorable**.
Unproven	Symantec does not have enough information about the file to assign a trust level to the file.
Poor	Symantec has only a few indications that the file is not trusted.
Bad	Symantec has high indications that the file is not trusted.

Norton Internet Security also provides different profiles to configure your scan performance. When you use the **Full Scan** profile, Norton Internet Security

follows the Blacklist technique to scan your computer. It scans all of the files on your computer against the signatures that it obtained during definition updates. When you use the **Standard Trust** or **High Trust** profile, Norton Internet Security follows the Whitelist technique to scan the files based on their confidence level. This way, Norton Internet Security significantly reduces the time that is required to scan your computer completely for security threats.

The Whitelist technique that Norton Insight uses also helps in heuristic detection of suspicious applications. Normally, the execution behavior of well-known applications appears identical to the execution behavior of unknown applications. Such behavior results in false identification of good applications as suspicious, and therefore, necessitates security applications to maintain a low heuristic detection threshold. However, keeping a low detection threshold does not provide a complete heuristic protection against malicious applications. Norton Internet Security uses the Whitelist technique that helps maintain a high heuristic detection threshold. It excludes well-known applications from heuristic detection to prevent false detection of well-known applications and to ensure a high detection rate of malicious applications.

Viewing the files using Norton Insight

Norton Insight provides information about the Files of Interest that are available on your computer. Norton Internet Security lets you view specific categories of files based on the option that you select in the **Norton Insight - Application Ratings** window.

The drop-down list that is available in the **Norton Insight - Application Ratings** window provides you the following options:

All Running Processes	Lists the processes that run on your computer at that point in time when you selected this option
All Files	Lists the Files of Interest
Startup Items	Lists the programs that start when you start your computer
All Loaded Modules	Lists all the files and programs that are currently loaded on to the program memory space
Highest Performance Impact	Lists the programs that consume maximum resources of your computer Norton Internet Security displays a list of top 10 resources that highly affect the performance of your computer.
Highest Community Usage	Lists the files that have the maximum community usage
Most Recently Discovered	Lists the files that you installed most recently The list contains the files that you installed in the last 30 days after you installed Norton Internet Security.

User Trusted Files	Lists the Files of Interest that you manually trusted in the **File Insight** window This category does not list the files that do not belong to the File of Interest even if you manually trust the files. However, Norton Internet Security excludes all of the manually trusted files from Norton Internet Security scan when you configure **Scan Performance Profiles** to **High Trust**. You can also remove the user trust from all of the Files of Interest that you manually trusted. You can use the **Clear All User Trust** option next to the drop-down list to remove the user trust.
Untrusted Files	Lists the files that are not Norton Trusted. You can manually trust all the files that are not trusted by clicking the **Trust All Files** option next to the drop-down list.

You can view file details such as file name, trust level, community usage, resource usage, and the stability rating. There may be instances when the trust level of a file has changed or a process running might have stopped running. You can refresh the **Norton Insight - Application Ratings** window to update the file list and file details. The coverage meter provides a graphical representation of the percentage of the Norton Trusted Files and the total Files of Interest. The higher the percentage, the lesser time the scan takes.

To view the files using Norton Insight

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **Application Ratings**.
3. In the **Norton Insight - Application Ratings** window, select an option from the drop-down list to view a category of files.
   You may need to scroll the window to view all the files that are listed in the details area.
4. Click **Close**.

To refresh the list of files

- In the **Norton Insight - Application Ratings** window, at the top of the file icon, click the **Refresh** icon.

Checking the trust level of a file

Norton Insight lets you check the details of the Files of Interest that are available on your computer. You can view details such as signature of the file and the date on which the file was installed. You can also view details such as the trust level, stability details, community usage, resource usage, and the source of the file. You can use the **Locate** option to find the location of the file on your computer. When you right-click a file that is available on your computer, the shortcut menu displays **Norton Internet Security** option and then **Norton File Insight** option. You can use the options to check the details of a File of Interest.

Norton Internet Security displays the **Norton File Insight** option only when you right-click a File of Interest. In Windows Safe mode, you cannot access this option for any file. Norton Internet Security also categorizes any file for which you open the **File Insight** window to view details as a File of Interest.

The Symantec server stores the hash value and trust level details of the File of Interest. The server provides the file details immediately after you open the **Norton**

Insight - Application Ratings window. However, you can use the **Check Trust Now** option in the **File Insight** window to update the trust value of a file. You can also manually trust any well-known files. You can change the trust level of any file to **User Trusted** other than the files that are Norton Trusted.

You can determine the resource usage of a file that is available on your computer. The **File Insight** window displays the CPU graph and the system resource usage details for the running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage or memory usage by the process.

To check the trust level of a file

1. In the Norton Internet Security main window, click **Advanced**.
2. In the window that appears, in the **Computer Protection** pane, click **Application Ratings**.
3. In the **Norton Insight - Application Ratings** window, click a file for which you want to check the details.
4. In the **File Insight** window, view the details of the file.
5. Click **Close** to close the **File Insight** window.

To check the trust level of a specific file

1. In the Norton Internet Security main window, click **Advanced**.
2. In the window that appears, in the **Computer Protection** pane, click **Application Ratings**.
3. In the **Norton Insight - Application Ratings** window, click **Check a Specific File**.
4. Browse to the location of the file for which you want to check the details.
5. Select the file, and then click **Open**.
6. In the **File Insight** window, view the details of the file.
7. Click **Close** to close the **File Insight** window.

To find the location of the file

❖ In the **File Insight** window, click **Locate**.

To refresh the trust level of the file

❖ In the **File Insight** window, click **Check Trust Now**.

To manually trust the file

❖ In the **File Insight** window, in the **Details** tab, click **Trust Now**.
You can manually trust the files that are poor, unproven, or not Norton trusted.

To determine the resource usage of a process

1 In the **File Insight** window, in the left pane, click **Activity**.
2 In the **Show** drop-down list, do one of the following:
   - Select **Performance** to view the performance graph of the process.
   - Select **Performance Alert** to view the performance alert-related details of the process.
   - Select **Network** to view the network activities of the process.
   - Select **Run Key change** to include registry changes.

Configuring the Scan Performance Profiles

The **Scan Performance Profiles** settings let you configure how Norton Internet Security should scan your computer based on the digital signature and confidence level of the files. To make Norton Internet Security scans lighter, faster, and more effective, you can exclude from scans the files that have known digital signatures or high confidence levels.

You can configure the **Scan Performance Profiles** settings to do the following:

- Configure to **Full Scan** to perform a complete scan of your computer.

The complete scan includes a scan of all files on your computer irrespective of the confidence level or digital signature of the files.

- Configure to **Standard Trust** to perform a scan that excludes the files that are Norton Trusted.

  Norton Internet Security scans the files that have a confidence level other than Norton Trusted.
- Configure to **High Trust** to perform a scan that excludes the files that have known digital signatures or high confidence levels.

  Norton Internet Security does not scan the files that have confidence level as Norton Trusted or User Trusted. It also excludes the Good files with high confidence level from the scan. It scans the files with confidence levels as Poor Trust, Unproven Trust, Bad Trust, and the files without a class 3 digital signature.

You must configure the **Scan Performance Profiles** settings before you run a scan or before a scan is scheduled to run. Norton Internet Security scans your computer according to the configuration you specified in the **Scan Performance Profiles** settings.

To configure Scan Performance Profiles from the Settings window

1. In the Norton Internet Security main window, click **Settings**.
2. In the Settings window, in the left pane, click **Computer Scan**.
3. In the **Scan Performance Profiles** row, click on one of the settings. Your options are:
   - **Full Scan**
   - **Standard Trust**
   - **High Trust**
4. Click **Apply**, and then click **OK**.

To configure Scan Performance Profiles from the Norton Insight - Application Ratings window

1. In the Norton Internet Security main window, click **Advanced**.
2. In the window that appears, in the **Computer Protection** pane, click **Application Ratings**.
3. In the **Norton Insight - Application Ratings** window, move the **Scan Performance Profiles** slider to one of the settings. Your options are:
   - **Full Scan**
   - **Standard Trust**
   - **High Trust**
4. Click **Close**.

About Monthly Report

Monthly Report lets you view a summary of what Norton Internet Security has done for you. Norton Internet Security displays the monthly report every 30 days after you install your product. After 30 days of installation, Norton Internet Security displays the Monthly Report automatically. If you do not want Norton Internet Security to display the Monthly Report automatically, you can select the **Do not display monthly reports automatically** option in the **Norton Monthly Report** window.

To turn on the **Monthly Report** option, go to the Norton Internet Security main window, and then click **Settings > General > Other Settings > Monthly Report > On**. The **Norton Monthly Report** window displays the **Tip of the month** to recommend some of the product's features and services.

When your product expires after the trial period, Monthly Report displays the activation status of your product. However, when your product expires after the subscription period, Monthly Report displays the subscription status of your product.

Norton Internet Security provides reports based on the following categories:

Computer	Lets you view the details of the various attacks your computer is protected from For example, you can view the total number of viruses and spyware from which you are protected.
Network	Lets you view the various types of Internet attacks from which you are protected For example, you can view the total number of intrusion attempts that are blocked.
Web	Lets you view the details of Antiphishing activities For example, you can view the total number of known authenticated sites that you visited.

Monthly Report lets you view the latest news on Internet security and also provides information on how to stay safe while you are online. You can click **Read More** in the **Norton Monthly Report** window to view more information on how to stay safe online.

Viewing the Monthly Report

The Monthly Report provides you with the statistics that are up to date. At a glance, you can see what Norton Internet Security has done for you since installation.

To view the Monthly Report

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Other Settings**.
4. In the **Monthly Report** row, click **View Report**.
5. View the report and click **Close**.

Protecting your files and data

3

This chapter includes the following topics:

- About maintaining protection
- About the Norton Internet Security scans

About maintaining protection

After you have installed your product and run LiveUpdate, you have complete protection from viruses and other security risks. However, new security risks are a constant threat. Security risks can spread when you start your computer from an infected disk or when you run an infected program. You can do several things to avoid security risks.

Practicing regular file maintenance and keeping your security protection up to date helps in protecting your computer.

To avoid security risks:

- Stay informed about the latest viruses and other security risks by logging in to the Symantec Security Response Web site at the following URL:

  http://securityresponse.symantec.com

  The Web site includes extensive, frequently updated information on viruses and automatic virus protection.
- Keep **Automatic LiveUpdate** turned on at all times to continually receive definition updates.

- Run LiveUpdate regularly to receive new program updates.
- Keep **Auto-Protect** turned on at all times to prevent viruses from infecting your computer.
- Watch for email messages from unknown senders. Do not open attachments from these senders.
- Keep **Email Protection** turned on to avoid sending or receiving infected email attachments.
- Keep all recommended maximum protection settings turned on.
- Keep the default options turned on at all times.

You should be always prepared in case a virus infects your computer.

Ensuring that protection settings are turned on

Norton Internet Security is configured to provide your computer with complete protection against viruses.

In addition, Norton Internet Security protects your computer against spyware, adware, and other security risks.

The default settings provide complete protection for your computer. However, you should ensure that your protection features are turned on for maximum protection.

To ensure that protection settings are turned on

1. In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, in the **Computer** tab, move the **On/Off** switch to the left to the **On** position for the following settings:

Computer Scan	Computer Scan provides the following options: **Compressed Files Scan** **Intelligent Skip Scanning** **Remove Infected Compressed Files** **Microsoft Office Automatic scan** **Rootkits and Stealth Items Scan** **Network Drives Scan**
Real Time Protection	Real Time Protection provides the following options: **Antispyware** **Auto-Protect** **Caching** **Removable Media Scan** **SONAR Protection**
Updates	Updates provides the following options: **Automatic LiveUpdate** **Pulse Updates** **Smart Definitions**

3 In the **Settings** window, click the **Network** tab.

4 In the **Intrusion Prevention** section, in the **Intrusion Prevention** row, move the **On/Off** switch to the left to the **On** position.

5 In the **Smart Firewall** section, in the **Smart Firewall** row, move the **On/Off** switch to the left to the **On** position.

6 In the **Message Protection** section, move the **On/Off** switch to the left to the **On** position, click **Configure**, and check all options for the following features:

Email Antivirus Scan	Email Antivirus Scan provides the following options: ▪ **Scan incoming email messages** ▪ **Scan outgoing email messages** ▪ **Scan outgoing messages for suspected worms** ▪ **Protect against timeouts** ▪ **Display progress indicator**
Instant Messenger Scan	You should configure any new instant messenger programs that you installed after you installed Norton Internet Security. ▪ Select the instant messenger clients that you want to protect.

7 In the **Settings** window, click the **General** tab.

8 In the left pane, click **Other Settings**.

9 In the **Insight Protection** row, move the **On/Off** switch to the left to the **On** position.

10 Click **Apply**, and then click **OK**.

About the Norton Internet Security scans

Norton Internet Security scans secure your computer from all types of viruses and unknown threats using the latest virus definitions. It also scans all the Internet

activities that are performed on your computer to protect your computer from the Internet-based threats that exploit software vulnerabilities.

Norton Internet Security automatically performs different types of scans to secure your computer from latest threats. It also lets you run different types of scans manually to secure your computer.

By using Norton Internet Security, you can run the following types of scans:

Computer Scan	**Computer Scan** uses the latest virus definitions that are available locally in the computer. If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer. The three types of scans that are available under **Computer Scan** are **Quick Scan**, **Full System Scan**, and **Custom Scan**.

Insight Network Scan	**Insight Network Scan** uses the virus definitions that are available locally and hosted in the Cloud. **Insight Network Scan** detects the files that are suspicious or vulnerable on your computer using the reputation-based threat detection. Norton Internet Security performs an **Insight Network Scan** only when the **Insight Protection** option is turned on. By default, the **Insight Protection** option is turned on. To turn on the **Insight Protection** option, go to the Norton Internet Security main window, and then click **Settings > General > Other Settings > Insight Protection > On**.

Reputation Scan	**Reputation Scan** displays the reputation information of the files on your computer. It displays the reputation information such as trust level, prevalence, stability rating, and resource usage. **Reputation Scan** displays the detailed reputation information of the good files and the number of bad files that have been detected or removed. **Reputation Scan** also internally performs **Computer Scan** and **Insight Network Scan** to detect the threats. The different types of scans that are available under Reputation Scan are **Quick Scan**, **Full System Scan**, and **Custom Scan**. Norton Internet Security Reputation Scan is applicable only for the executable files and the installer files.

Scan Facebook Wall	**Scan Facebook Wall** lets you scan the links and URLs that are available on your Facebook profile. When you click the **Scan Facebook Wall** option, Norton Internet Security takes you to the Facebook login Web page. After you log in to your Facebook profile, Norton Safe Web asks you to grant permission to access your Facebook wall. To do so, use the **grant us permission to access your stream** option available on the Facebook Web page, and then follow the on-screen instructions. After you grant permission, Norton safe Web scans all the available links on your Facebook wall each time you use **Scan Facebook Wall** option. It then displays the security status of the scanned URLs.

Norton Internet Security also performs **Idle Time Scans**. **Idle Time Scans** detect the time when you are not using your computer and intelligently run scans depending on the scan history of your computer. Norton Internet Security keeps your computer secure from latest threats by automatically running scans on your computer by using the Idle Time Scans feature. You can use **Idle Time Scans** to protect your computer against virus infections without compromising the performance of your computer. **Idle Time Scans** automatically detect the idle state of your computer and runs a Quick Scan or a Full System Scan.

Norton Internet Security provides options to configure Norton Internet Security scans. The computer settings

and some of the options in the network settings let you configure how you want Norton Internet Security to scan your computer for viruses and other security threats. You can click the **Settings** link available in the Norton Internet Security main window and view the options that are available under the **Computer** tab and **Network** tab.

Accessing Norton Internet Security scans

You can use Norton Internet Security scans to secure your computer from all types of viruses and unknown threats.

You can access Full System Scan and custom scans from the Norton Internet Security main window. You can access Quick Scan from the Norton Internet Security main window or the Norton Internet Security icon on the taskbar.

You can also scan any particular folder using the context scan feature. The context menu scan is available when you right-click the folder that you want to scan.

If the **Insight Protection** option is turned on, when you right-click a file, the shortcut menu displays Norton Internet Security and then **Insight Network Scan**. You can use this command to scan a file using both the local definitions and the definitions that are hosted in the Cloud.

You can also run the Reputation Scan to view the reputation information of the files.

To access the scan from the Norton Internet Security main window

1 In the Norton Internet Security main window, in the **Computer Protection** pane, click **Scan Now**.

2 In the window that appears, do one of the following:
- In the **Computer Scan** pane, click the scan that you want to run.
- Click **Reputation Scan**, and then click the scan that you want to run.
- Click **Scan Facebook Wall** to scan the links that are available on your Facebook wall.

To access the scan from the notification area

❖ In the notification area on the taskbar, right-click the Norton Internet Security icon, and then click **Run QuickScan**.
By default, **Insight Protection** option is turned on. In this case, Norton Internet Security performs an Insight Network Quick Scan simultaneously with a traditional Quick Scan.

To scan a particular folder

❖ Right-click the folder, and click Norton Internet Security > **Scan Now**.

To scan a particular file

❖ Right-click the file, and click Norton Internet Security > **Insight Network Scan**.
The **Insight Network Scan** option is available only if the **Insight Protection** option is turned on. To access the **Insight Protection** option, go to the Norton Internet Security main window, and then click **Settings > General > Other Settings > Insight Protection**.

About Computer Scan

Norton Internet Security automatically downloads latest virus definition regularly and secures your computer from all types of viruses and unknown threats. When Norton Internet Security performs a Computer Scan, it uses the latest virus definitions that Symantec provides.

The threat detections that are based on the local definition are specified with a specific name. For

example, if a Trojan horse is detected, the scan results of the Computer Scan displays the threat as Trojan.Foo. You can click the **Scan Now** option available in the Norton Internet Security main window to access the different types of computer scans.

If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer.

You can run the following types of computer scans:

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. **Quick Scan** takes less time to scan than a Full System Scan because this scan does not scan your entire computer.
Full System Scan	Scans your computer for all types of viruses and security threats. **Full System Scan** performs a deep scan of your computer to remove viruses and other security threats. It checks all boot records, files, and running processes to which the user has access. Consequently, when you run a Full System Scan with administrator privileges, it scans more files than when you run it without administrator privileges. Full System Scan scans all the local drives, mapped network drives, and removable drives except floppy drives. You can also minimize and run a **Full System Scan** in the background.

Custom Scan	Scans a particular file, removable drives, any of your computer's drives, or any folders or files on your computer. You can create a custom scan if you regularly scan a particular location of your computer. Norton Internet Security lets you scan this location frequently without having to specify it every time. You can also schedule the custom scan to run automatically.

Computer Scan provides details about the scanned items. You can view the details such as total number of files scanned, security risks detected, security risks resolved, and the total items that require attention. It also provides you the different ways to resolve any items that were not automatically resolved during the scan. You can also view the severity of the risk, the name of the risk, and the status of the risk about the resolved items.

Running a Full System Scan

Full System Scan performs a deep scan of the system to remove viruses and other security threats. It checks all boot records, files, and running processes to which the user has access. Consequently, when you run a **Full System Scan** with administrator privileges, it scans more files than when you run it without administrator privileges.

You can also minimize and run a **Full System Scan** in the background.

To run a Full System Scan

1 In the Norton Internet Security main window, click **Scan Now**.

2 In the **Computer Scan** pane, click **Full System Scan**. You can use the following options to suspend a **Full System Scan**:

Pause	Suspends a **Full System Scan** temporarily. Click **Resume** to continue the scan.
Stop	Terminates a **Full System Scan**. Click **Yes** to confirm.

3 On the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If any items require attention, review the risks on the **Threats Detected** window.

Running a Quick Scan

Quick Scan is a fast scan of the areas of your computer that the viruses and other security risks often target. Because this scan does not scan your entire computer, it takes less time to run than a **Full System Scan**.

When the **Insight Protection** option is turned on, Norton Internet Security simultaneously performs a traditional Quick Scan and an Insight Network Quick Scan. By default, the **Insight Protection** option is turned on.

To run a Quick Scan

1 In the Norton Internet Security main window, click **Scan Now**.

2 In the **Computer Scan** pane, click **Quick Scan**. You can use the following options to suspend a **Quick Scan**:

Pause	Suspends a **Quick Scan** temporarily. Click **Resume** to continue the scan.
Stop	Terminates a **Quick Scan**. Click **Yes** to confirm.

3 On the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If any items require attention, review the risks on the **Threats Detected** window.

Scanning selected drives, folders, or files

Occasionally, you might want to scan a particular file, removable drives, any of your computer's drives, or any folders or files on your computer. For example, when you work with removable media and suspect a virus, you can scan that particular disk. Also, if you have received a compressed file in an email message and you suspect a virus, you can scan that individual element.

To scan individual elements

1 In the Norton Internet Security main window, click **Scan Now**.

2 In the **Computer Scan** pane, click **Custom Scan**.

3 In the **Scans** window, do one of the following:

- To scan specific drives, click **Run** next to **Drive Scan**, select the drives that you want to scan, and then click **Scan**.
- To scan specific folders, click **Run** next to **Folder Scan**, select the folders that you want to scan, and then click **Scan**.
- To scan specific files, click **Run** next to **File Scan**, select the files that you want to scan, and then click **Add**.

  You can also press **Ctrl**, and select multiple files to scan.

  You can use the following options to suspend a scan:

Pause	Suspends a custom scan temporarily. Click **Resume** to continue the scan.
Stop	Terminates the scan. Click **Yes** to confirm.

4 In the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If any items require attention, review them on the **Threats Detected** window.

About the Results Summary window

Norton Internet Security displays the **Result Summary** window when you run a manual scan. At the end of a scan, the **Results Summary** window provides the summary of the scan results.

If your most recent scan was a Quick Scan, this window shows the results of a fast scan of the areas of your

computer. Viruses, spyware, and other risks often target these areas.

If your most recent scan was a Full System Scan, this window shows the results of a comprehensive scan of your entire computer.

The **Result Summary** window displays the following information:

- Total items scanned
- Total security risks detected
- Total security risks resolved
- Total items that require your attention

About the Threats Detected window

Norton Internet Security displays the **Threats Detected** window when it detects threats. At the end of a scan, the **Threats Detected** window provides you different ways to resolve any items that were not automatically resolved during the scan.

The **Threats Detected** window provides the information such as the severity of the risk, the name of the risk, and the status of the risk. It also provides the action that you can take to resolve the item. The **Threats Detected** window provides you the different options such as **Fix**, **Manual Fix**, **Exclude**, **Get Help**, and **Rescan** to resolve the item.

It also provides the **Ignore** option only once during the first-time detection of low-risk items.

Ignore option is available once until you do not change the default settings for the **Low Risks** option under **Computer Scan**.

The options in the **Threats Detected** window vary based on the types of files that Norton Internet Security identified as infected during the scan.

About custom scans

You can create a custom scan if you regularly scan a particular segment of your computer. This custom scan lets you scan the segment frequently without having to specify it every time. You can also schedule the custom scan to run automatically on specific dates and times or at periodic intervals. You can schedule a scan according to your preferences. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work.

You can delete the scan when it is no longer necessary. For example, if you work on a project for which you need to swap files frequently with others. In this case, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

Creating a custom scan

Instead of running the default scans that are listed in the **Scans** pane, you can create your own scans that meet your specific requirements. For example, you can create a scan that checks a folder in which you store all the downloaded files.

You can create a custom scan in the **Scans** window.

When you create custom scans, you can also schedule them to run automatically on specific dates and times or at periodic intervals.

To create a custom scan

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the **Computer Scan** pane, click **Custom Scan**.
3. In the **Scans** window, click **Create Scan**.
4. In the **New Scan** window, in the **Scan Name** box, type a name for the scan.
5. On the **Scan Items** tab, add the items that you want to scan. See "Selecting the scan items" on page 124.

6 On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 128.
7 On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 125.
8 Click **Save**.

Selecting the scan items

When you configure a custom scan, you must select the items that you want to include in the scan. You can include individual files, folders, or drives. You can include multiple drives, folders, and files to add to the scan. You can also exclude items from the scan.

When you select a drive, all the items in the drive including the files and folders are automatically added to the scan. When you select a folder, all of the files in folder are added to the scan.

To select the scan items

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, do one of the following:
- To add items for a new scan, click **Create Scan**.
  You must provide a name for the scan in the **Scan Name** box.
- To add items for an existing scan, in the **Edit Scan** column, click the edit icon for the scan that you want to modify.

4 In the window that appears, on the **Scan Items** tab, do the following:
   - To add drives, click **Add Drives**, in the **Scan Drives** dialog box, select the drives to be scanned, and click **Add**.
   - To add folders, click **Add Folders**, in the **Scan Folders** dialog box, select the folders to be scanned, and click **Add**.
   - To add files, click **Add Files**, in the **Files to Scan** dialog box, select the files to be scanned, and then click **Add**.

   If you need to remove an item from the list, select the item, and then click **Remove**.
5 Click **Save**.

Configuring the scan options

Norton Internet Security lets you configure scan options for each scan that you create. By default, the scan options reflect the current **Computer Scan** settings in the **Settings** window. The changes that you make are applicable to the current scan only. Any change that is made to the **Computer Scan** settings in the **Settings** window does not affect the scan options settings for the current scan.

In addition to the custom scans that you create, you can also configure the scan options for the default scans. You can configure scan options for Full System Scan, Quick Scan, Drive Scan, Folder Scan, and File Scan.

To configure the scan options

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the scan that you want to schedule.

4 In the **Edit Scan** window, on the **Scan Options** tab, configure the scan options as required.
5 Click **Save**.

Editing a custom scan

You can edit a custom scan that you created. You can include additional files or folders to the scan or remove the files and folders that you do not want to scan. You can also change the name of the scan.

You can edit a custom scan in the **Scans** window.

To edit a custom scan

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the custom scan that you want to modify.
4 In the **Edit Scan** window, on the **Scan Items** tab, select the items that you want to scan. See "Selecting the scan items" on page 124.
5 On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 128.
6 On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 125.
7 Click **Save**.

Running a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

You can run a custom scan from the **Scans** window.

To run a custom scan

1 In the Norton Internet Security main window, click **Scan Now**.

2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, click **Run** next to the custom scan that you want to run.
You can use the following options to suspend a custom scan:

Pause	Suspends a custom scan temporarily. Click **Resume** to continue the scan.
Stop	Terminates a custom scan. Click **Yes** to confirm.

4 In the **Results Summary** window, do one of the following:
- If no items require attention, click **Finish**.
- If any items require attention, review the risks on the **Threats Detected** window.

Deleting a custom scan

You can delete custom scans if they are no longer needed.

You can delete a custom scan in the **Scans** window.

To delete a custom scan

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, in the **Delete** column, click the delete icon next to the custom scan that you want to delete.
4 Click **Yes** to confirm that you want to delete the scan.

About scheduling scans

Norton Internet Security uses Idle Time Scans to automatically detect the idle state of your computer and runs a Full System Scan when the computer is idle. However, you can schedule a Full System Scan according to your preferences. Norton Internet Security prompts you that the **Idle Time Scans** option gets turned off when you schedule a Full System Scan. You can also set up a schedule for a Quick Scan and custom virus scans.

You can schedule scans to run automatically on specific dates and times or at periodic intervals. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work. Norton Internet Security lets you schedule the Full System Scan, Quick Scan, and custom virus scans. However, you cannot schedule the Drive Scan, Folder Scan, and File Scan.

You can also set up Norton Internet Security to turn off your computer automatically when the scheduled scan is complete.

Scheduling a scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (daily, weekly, or monthly), you are presented with additional options. For example, you can request a monthly scan, and then schedule it to occur on multiple days instead.

In addition to the custom scans that you create, Norton Internet Security lets you schedule the Full System Scan and Quick Scan.

You can also schedule the scan to run in specific time intervals (hours or days). You can schedule a custom scan in the **Scans** window.

Norton Internet Security lets you select multiple dates if you are scheduling a monthly scan.

To schedule a custom scan

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the **Computer Scan** pane, click **Custom Scan**.
3 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the custom scan that you want to schedule.
4 In the **Edit Scan** window, on the **Scan Schedule** tab, do one of the following:
   - To run the scan at specific time intervals, select **Run at specific time interval**.
   - To run the scan at specific time every day, select **Daily**.
   - To run the scan on a specific day on a week, select **Weekly**.
   - To run the scan on a specific day on a month, select **Monthly**.

   These frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
5 Under **Run the scan**, do the following:
   - To run the scan only at idle time, check **Only at idle time**.
   - To run the scan only when your computer is connected with external power source, check **Only on AC power**.
   - To prevent your computer from going to a Sleep or Standby mode, check **Prevent standby**.
6 Under **After scan completion:**, select the state at which your computer should be after the scan is complete. Your options are:
   - **Stay On**
   - **Turn Off**
   - **Sleep**
   - **Hibernate**
7 Click **Save**.

Scheduling a Full System Scan

Norton Internet Security uses **Idle Time Scans** to automatically detect the idle state of your computer. Norton Internet Security runs a weekly **Full System Scan** when the computer is idle. The **Full System Scan** protects your computer against infection without compromising the performance of your computer. You can override the **Idle Time Scans** settings to schedule a **Full System Scan** on specific dates and times or at periodic intervals. However, before you schedule a **Full System Scan**, you need to turn off the **Idle Time Scans** option.

You can schedule a **Full System Scan** in the **Scans** window.

The **Idle Time Scans** option provides sufficient protection to your computer by running a **Full System Scan** when your computer is idle. Symantec recommends you not to turn off the **Idle Time Scans** option.

To schedule a Full System Scan

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the **Computer Scan** pane, click **Custom Scan**.
3. In the **Scans** window, in the **Edit Scan** column, click the edit icon next to **Full System Scan**.
4. In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
5. Click **Save**.

Scheduling a Quick Scan

Quick Scan scans the important locations of your computer that the viruses and other security threats often target. When you perform a Quick Scan, Norton

Internet Security scans only the running processes and the loaded programs. Quick Scan takes less time to scan than a Full System Scan because this scan does not scan your entire computer.

Norton Internet Security lets you schedule a Quick Scan. You can schedule a Quick Scan in the **Scans** window.

To schedule a Quick Scan

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the **Computer Scan** pane, click **Custom Scan**.
3. In the **Scans** window, in the **Edit Scan** column, click the edit icon next to **Quick Scan**.
4. In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
5. Click **Save**.

Editing a scheduled scan

You can change the schedule of any scheduled custom scan, **Quick Scan**, or **Full System Scan** from the **Scans** window.

To edit a scheduled scan from Norton Internet Security Scans dialog box

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the **Computer Scan** pane, click **Custom Scan**.
3. In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the scan that you want to edit..
4. In the **Edit Scan** window, on the **Scan Schedule** tab, change the schedule as required.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.

5 Click **Save**.

Running a scan at the command prompt

You can scan with Norton Internet Security from the command prompt without opening the Norton Internet Security main window. You type the path and name of the file that you want to scan or customize the scan by adding a specific command. The following commands are available:

/?	NAVW32 launches help and terminates.
/A	Scans all drives
/L	Scans the local drives
/S[+|-]	Enables (+) or disables (-) subfolders scanning
/B[+|-]	Enables (+) or disables (-) boot record scanning and master boot record scanning (for example, NAVW32 C: /B+ or NAVW32 C: /B-)
/BOOT	Scans only the boot records
/QUICK	Runs a Quick Scan
/SE[+|-]	Enables (+) or disables (-) a Quick Scan

/ST[+|-]	Enables (+) or disables (-) scanning of stealth items
/TASK:[taskfile.sca]	Uses a task file as input to the list of items to scan Task file path should follow the ':' (for example, TASK:C:\Documents and Settings\All Users\Application Data\Symantec\Norton Internet Security\Tasks\Full.sca)
/TTASK:[taskfile.sca]	Uses a task file as input to the list of items to scan Task file path should follow the ':' (for example, TASK:C:\Documents and Settings\All Users\Application Data\Symantec\Norton Internet Security\Tasks\Full.sca) Assumes the task file as a temporary file and deletes the task file at the end of processing.
[folder_path]*[?]	Scans the files that matches specified wild card

[drive|folder|file]	Scans the specified drive, folder, or file
/SESCAN	Performs Quick Scan in the background. Norton Internet Security displays the **scans** window only when a threat is detected.

To run a scan from the command prompt

1 At the command prompt, type the path in which Norton Internet Security is located and the executable's file name.
The following examples show the syntax of a scan command:

- **`"\Program Files\Norton Internet Security\Engine\version\NAVW32" /command_name`**
  Where *version* represents the version number of Norton Internet Security and *command_name* represents the command.
- **`"\Program Files\Norton Internet Security\Engine\version\NAVW32" [path]file_name`**
  Where *version* represents the version number of Norton Internet Security and *[path]file_name* represents the location, name, and extension of the file.

2 Press **Enter**.

About Insight Network scan

The Insight Network scan uses the Cloud technology wherein a remote server on the Web contains the latest virus definitions. Norton Internet Security scans your computer for the latest security threats. When Norton

Internet Security performs the Insight Network scan, it uses the virus definitions that are available locally and in the Cloud. Norton Internet Security provides additional protection by using the most recent definitions in the Cloud, apart from the definitions that are available locally on your computer.

Norton Internet Security performs an Insight Network scan only when the **Insight Protection** option is turned on. To turn on the **Insight Protection** option, go to the Norton Internet Security main window, and then click **Settings > General > Other Settings > Insight Protection > On**. By default, the **Insight Protection** option is turned on.

When the **Insight Protection** option is turned on, Norton Internet Security performs a traditional scan and an Insight Network scan simultaneously. The traditional scan uses the definitions from the local system, and the Insight Network scan uses the definitions that are hosted in the Cloud.

Threat detection based on the Cloud definitions is identical to the threat detection that is based on the local definitions. However, the Cloud definitions are specified with additional data about the threats that it detects which indicates that it has been obtained from the Internet. Definitions in the Cloud provide a generic name for the risk detected, but the local definitions provide the specific name for the risk detected. For example, if a Trojan horse is detected, the scan results of the Insight Network might display Cloud.Trojan. However, the scan results of the local definition might display Trojan.Foo.

If the traditional scan completes while the Insight Network scan is still running, you can view the **Insight Network Scan** progress status.

If the **Insight Protection** option is turned on, you can manually run the following types of Insight Network scans:

- Insight Network Quick Scan

Norton Internet Security simultaneously performs a traditional Quick Scan and an Insight Network Quick Scan to scan the areas of your computer that the viruses often target. Norton Internet Security also performs an Insight Network Quick Scan simultaneously with an Idle Quick Scan.

- Insight Network Single File Scan

  Norton Internet Security simultaneously performs a traditional Single File Scan and an Insight Network Single File Scan to scan a file on your computer. It also scans the files that are received through instant messenger programs. You can perform this scan by running an Insight Network scan on single file using the **Custom Scan** option on the **Scans** window.

- Insight Network context-menu scan

  When you right-click a file, the shortcut menu displays Norton Internet Security and then **Insight Network Scan**. You can use this command to scan a file using both local definitions and definitions that are hosted in the Cloud.

This **Insight Network Scan** command is available only for single file.

Turning off or turning on Insight Protection

Insight Protection option lets Norton Internet Security perform an Insight Network scan on your computer

When the **Insight Protection** option is turned on, Norton Internet Security performs a traditional scan and an Insight Network scan simultaneously. The traditional scan uses the definitions from the local system, and the Insight Network scan uses the definitions that are hosted in the Cloud. Norton Internet Security performs only a traditional scan if the **Insight Protection** option is turned off.

Norton Internet Security performs an Insight Network scan only when the **Insight Protection** option is turned

on. By default, the **Insight Protection** option is turned on.

To turn off or turn on the Insight Protection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Other Settings**.
4. In the **Insight Protection** row, do one of the following:
   - To turn off Insight Protection, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Insight Protection, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.

About Reputation Scan

Reputation Scan provides information on the trust-worthiness of all programs and running processes on your computer. It helps you detect the files that are suspicious or vulnerable on your computer using the reputation-based threat detection. Norton Internet Security lets you run different types of Reputation Scan and detect suspicious programs on your computer.

Reputation Scan filters the files on the basis of certain filtering criteria and performs an **Insight Network Scan** on the filtered files. Reputation Scan filters the files as reputation files. It filters .exe files, .scr files, .sys files, .dll files, .drv files, .ocx files, .loc files, and .msi files and analyzes these files.

When you perform a Reputation Quick Scan or Full System Scan, Norton Internet Security considers the Files of Interest that are available on your computer.

After it has filtered the reputation files, Norton Internet Security performs an **Insight Network Scan**. When Norton Internet Security performs an **Insight Network Scan**, it also performs a **Computer Scan**. Norton Internet Security uses the **Computer Scan** to perform

the signature-based threat detection. It compares the signature of the filtered reputation files against the known threat signatures to identify threats on your computer. If a security threat is detected, Norton Internet Security automatically removes the threat from your computer.

Norton Internet Security uses the **Insight Network Scan** to detect suspicious or vulnerable files on your computer using the reputation-based threat detection. The **Insight Network Scan** uses the Cloud technology wherein a remote Symantec server on the Web stores the latest reputation information. It checks the Cloud for the reputation information on the filtered files.

Norton Internet Security obtains specific information such as file name and hash key about the filtered reputation files and sends this information to the Cloud. The Cloud analyzes the file information and provides a trust level for each file. The Symantec server sends back the reputation information to your computer. If any of the filtered files is suspicious or vulnerable, Norton Internet Security assigns **Bad** or **Poor** trust level. Apart from reputation information, Norton Internet Security also checks for the latest virus definitions on the Cloud.

Your computer must be connected to the Internet to access the latest reputation information and virus definitions from the Cloud. If your computer is not connected to the Internet, Norton Internet Security uses the reputation information that is available locally.

When you perform a Reputation Scan, Norton Internet Security considers only the following categories of files:

Executable files	This category includes Windows executable files (.exe) and script files (.scr).

System files	This category includes Windows System files (.sys), dynamic link library files (.dll), and device driver files (.drv).
Developer files	This category includes ActiveX control files (.ocx).
Miscellaneous files	This category includes Windows Installer Package files (.msi) and resource-only DLL files (.loc).

Norton Internet Security lets you scan specific areas of your computer based on the type of Reputation Scan that you select. You can manually run the following types of Reputation Scan:

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. When you perform a Quick Scan, Norton Internet Security considers the Files of Interest that related to loaded programs and the running processes.

Full System Scan	Scans all the Files of Interest that are available on your computer. When you perform a Full System Scan, Norton Internet Security searches for Files of Interest on all the locations on your computer. The locations include all drives, running processes, loaded programs, and startup files.
Custom Scan	Scans a specific file, folder, drive, or removable drive. When you perform a custom scan, Norton Internet Security considers only the filtered reputation files.

Symantec rates a file based on the statistical evaluation that is done on the file using the Norton Community Watch data and Symantec's analysis. Symantec assigns the following confidence levels to reputation files:

Good	Symantec has a high indication that the file is trusted.
Unproven	Symantec does not have enough information about the file to assign a trust level to the file. The file is neither safe nor unsafe.

Poor	Symantec has a few indications that the file is not trusted. This file is suspicious and can harm your computer.
Bad	Symantec has a high indication that the file is not trusted. This file is suspicious and can harm your computer.

When the Reputation Scan is complete, you can view the summary of the scan results in the **Norton Reputation Scan** window. You can view the reputation information such as the file name, trust level, age of the file, stability rating, and community usage for each file. The trust level determines whether a file is safe or unsafe. If a file has **Poor** or **Bad** trust level, Norton Internet Security lets you quarantine the file.

Running a Reputation Full System Scan

When you perform a **Full System Scan**, Norton Internet Security scans all the Files of Interest that are available on your computer. This fileset includes the files that relate to the running processes, startup files, and loaded programs.

To run a Reputation Full System Scan

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the window that appears, click **Reputation Scan**.
3. In the **Reputation Scan** pane, click **Full System Scan**.
   In the **Norton Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.

4 If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
5 In the **Quarantine File** window, click **Quarantine this file**.
6 In the **Manual Quarantine** window, click **Add**.
7 Click **Close**.
8 In the **Norton Reputation Scan** window, click **Close**.

Running a Reputation Quick Scan

When you perform a **Quick Scan**, Norton Internet Security scans only the running processes and the loaded programs. Reputation Quick Scan does not scan your entire computer and it takes lesser time to run than a Reputation Full System Scan.

To run a Reputation Quick Scan

1 In the Norton Internet Security main window, click **Scan Now**.
2 In the window that appears, click **Reputation Scan**.
3 In the **Reputation Scan** pane, click **Quick Scan**. In the **Norton Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.
4 If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
5 In the **Quarantine File** window, click **Quarantine this file**.
6 In the **Manual Quarantine** window, click **Add**.
7 Click **Close**.
8 In the **Norton Reputation Scan** window, click **Close**.

Running a Reputation custom scan

Norton Internet Security lets you scan specific areas on your computer by using the Reputation custom scan. You can scan any of your computer's drives, removable drives, folders or files. For example, if you want to

check the trust level of a specific file, you can scan the particular file.

To run a Reputation custom scan

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the window that appears, click **Reputation Scan**.
3. In the **Reputation Scan** pane, click **Custom Scan**.
4. In the **Reputation Custom Scan** window, do one of the following:
   - Click **Drive Scan**, select the drive that you want to scan, and then click **Scan**.
   - Click **Folder Scan**, select the folder that you want to scan, and then click **OK**.
   - Click **File Scan**, select the file that you want to scan, and then click **Open**.

   In the **Norton Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.
5. If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
6. In the **Quarantine File** window, click **Quarantine this file**.
7. In the **Manual Quarantine** window, click **Add**.
8. Click **Close**.
9. In the **Norton Reputation Scan** window, click **Close**.

About the Reputation Scan results

Norton Internet Security lets you run different Reputation Scans to detect any suspicious programs or vulnerable programs on your computer. Norton Internet Security lets you manually run the following types of Reputation Scan:

- Reputation Quick Scan
- Reputation Full System Scan
- Reputation custom scan

When you run a Reputation Quick Scan, Norton Internet Security considers the Files of Interest which include running processes and loaded programs. When you run a Reputation Full System Scan, Norton Internet Security considers all the Files of Interest that are available on your computer. When you run a Reputation custom scan, Norton Internet Security lets you select the drive, folder, or file that you want to scan.

Reputation Scan filters the files on the basis of certain filtering criteria and performs an **Insight Network Scan** on the filtered files. Reputation Scan filters .exe files, .scr files, .sys files, .dll files, .drv files, .ocx files, and .msi files and analyzes these files.

Norton Internet Security displays the reputation information of the scanned files in the **Norton Reputation Scan** window.

Norton Internet Security consolidates the reputation information of your most recent scan and presents the reputation information using different graphical formats.

The top of the **Norton Reputation Scan** window displays the following statistics:

- The **Trust Level** graph displays the average trust level of files on your computer. It also displays the average trust level of the files that Symantec analyzes within the Norton Community.
- The **Prevalence** graph displays the average high user prevalence of files on your computer. It also displays the average high user prevalence of the files that Symantec analyzes within the Norton Community.
- The **Stability** graph displays the average reliable files on your computer. It also displays the average reliable files that Symantec analyzes within the Norton Community.

Stability ratings vary depending upon your operating system.

- The **Norton Network** graph displays the details about the known good files and bad files.

  You can view the number of trusted files that are on your computer. You can also view the total number of files that Symantec analyzes within the Norton Community.

Your computer must be connected to the Internet to view these details. Norton Internet Security connects to the Symantec servers to collect the reputation information.

The bottom of the **Norton Reputation Scan** window displays the reputation information of each scanned item. For each scanned item, you can view the following details:

File Name	Indicates the file name and file type. You can click a file name to view additional details about the file in the **File Insight** window.

Trust Level

Indicates the trust level that is assigned to a file.

Symantec analyzes specific information about a file such as the digital signature and the hash value to determine the trust level of a file. Symantec rates a file based on the statistical evaluation that is done on the file using the Norton Community Watch data and Symantec's analysis.

Symantec assigns the following trust levels to reputation files:

- **Trusted**: Symantec has a high indication that the file is trusted.
- **Good**: Symantec has a high indication that the file is trusted.
- **Unproven**: Symantec does not have enough information about the file to assign a trust level to the file.
- **Poor**: Symantec has a few indications that the file is not trusted.
- **Bad**: Symantec has a high indication that the file is not trusted.

If you have a file that has **Poor** or **Bad** trust level, Norton Internet Security displays a red cross (x) icon next to the trust level. You can click on the red cross (x) icon and quarantine the

	suspicious file.
Prevalence	Indicates the community usage level of the file. The search results are grouped in to the following categories: ■ **Very Few Users**: Shows the files that have very low user prevalence. ■ **Few Users**: Shows the files that have average user prevalence. ■ **Many Users**: Shows the files that have very high user prevalence. You can also use the community usage of a file to determine the legitimacy of the file. Symantec uses a stringent statistical method to evaluate the trustworthiness of a file and to classify the file as a Good file.

Resource Usage	Indicates the system resource usage level of the file. The usage levels are as follows: ■ **Low**: Indicates that the file consumes minimum system resources. ■ **Moderate**: Indicates that the file consumes moderate system resources. ■ **High**: Indicates that the file consumes maximum system resources. ■ **Unknown**: Indicates that the file has performed no action in your computer.

Stability	Indicates the stability rating of the file. The stability rating depends on how frequently the program crashes. The different stability ratings are as follows: ▪ **Reliable**: Indicates that the program is reliable. ▪ **Stable**: Indicates that the program is comparatively stable. However, it crashes sometimes. ▪ **Slightly Unstable**: Indicates that the program is slightly unstable. ▪ **Unstable**: Indicates that the program is unstable. ▪ **Very Unstable**: Indicates that the program frequently crashes. ▪ **Unknown**: Indicates that the crash history of the program is not known. Stability ratings vary depending upon your operating system.

About Scan Facebook Wall

Norton Safe Web protects your computer while you use Facebook. It scans each URL that is available on your Facebook Wall and displays the Norton rating icons for the scanned URLs.

You can also check if a URL is safe or unsafe and then share the URL with your friends on Facebook. Norton Safe Web scans the URL that you post on Facebook and gives you the safety status for the URL. This way, you

are not only protected from unsafe sites but you also let other Facebook users know the security status of any Web site.

However, Norton Safe Web requires your permission to scan the URLs that are available on your Facebook Wall. When you log in to Facebook, Norton Safe Web asks for your permission to access your Facebook Wall. You can choose to allow or deny permission to let Norton Safe Web access your Facebook Wall.

The auto-scan feature in Norton Safe Web application page helps you protect your Facebook Wall. Norton Safe Web scans the News Feed on your Facebook Wall periodically and protects you from malicious links. When Norton Safe Web detects a malicious link, it notifies you with a post on your Facebook Wall. To activate Norton Auto-Scan, go to your **Norton Safe Web** page on Facebook and click **Enable Auto-Scan**.

To remove the malicious link from your Facebook Wall, go to your profile and remove the malicious link. If your friend has posted the malicious link, you can use the **WARN YOUR FRIENDS** option in the message to alert your Facebook friend. You can also click **See Norton Safe Web Report** to view Norton ratings and other details about this malicious link. When no malicious activity is detected on your Facebook Wall, Norton Safe Web posts a message notifying that your Facebook Wall is safe. Norton Safe Web posts this message on your Facebook Wall once in every 30 days.

If you later decide to remove Norton Safe Web from your Facebook profile, you can use the **Application Settings** option of Facebook.

The following are the safety states that Norton Safe Web provides after it scans the links on your Facebook Wall:

Safe	Indicates that the site is safe to visit and Norton Trusted. The sites with this rating do not harm your computer and so you can visit this site.
Warning	Indicates that the site has security risks. The sites with this rating may install malicious software on your computer. Symantec recommends that you do not visit this site.
Untested	Indicates that Norton Safe Web has not yet tested this site and it does not have sufficient information about this site.
Caution	Indicates that the site may have security threats. Symantec recommends you to be cautious while you visit such Web sites.

Scanning your Facebook Wall

The Norton Safe Web feature scans your Facebook Wall and analyzes the security levels of all the available links on your Facebook Wall. It then displays the security status of the scanned URLs. However, Norton Safe Web requires your permission to scan your Facebook Wall.

To scan your Facebook Wall

1. In the Norton Internet Security main window, click **Scan Now**.
2. In the window that appears, click **Scan Facebook Wall**.
3. In the **Norton Safe Web for Facebook** pane, click **Scan Facebook Wall**.
4. In the Facebook login Web page, log in to your Facebook profile.
5. In the **Request for permission** page, click **Allow**.
6. In the Web page that appears, click **Please grant us permission to access your News Feed and Wall**.
7. Follow the on-screen instructions to let Norton Safe Web access your Facebook Wall.

About Idle Time Scans

Norton Internet Security keeps your computer secure from ongoing threats by automatically running scans on your computer by using the Idle Time Scans feature. Idle Time Scans detect the time when you do not use your computer and intelligently run scans depending on the scan history of your computer.

The **Idle Time Scans** option is automatically turned on when you install Norton Internet Security. Even though Idle Time Scans automatically run the scans, you can still customize the settings of **Idle Time Scans**. Norton Internet Security decides when to run Idle Time Scans, depending on your settings and a few other predefined parameters.

The following list provides details on the settings that you can make and the predefined parameters:

Idle Time Out duration	You can set the duration after which Norton Internet Security should identify your computer as idle. You can select a value (in minutes) between 1 minute and 30 minutes. When you do not use your computer for the duration that you specify, Norton Internet Security checks for the other predefined parameters and runs Idle Time Scans.
Predefined parameter	Some of the predefined parameters that Norton Internet Security checks are CPU idle time, disk usage, and type of electric current you use to operate your computer. For example, you set the Idle Time Out duration as 10 minutes and watch an online video for 11 minutes without any intervention. In this case, Idle Time Scans do not run because of the CPU-intensive task.

You must run your computer on alternating current (AC) power for Norton Internet Security to run Idle Time Scans.

You can view the results of the scans in any of the following locations:

- The Scan Results category in the **Security History** window
- The Norton Tasks category in the **Norton Tasks** window

Norton Internet Security discontinues any Idle Time Scans that it started during idle time if you begin to use your computer again. However, it resumes the scan when your computer is idle again.

You must turn off Idle Time Scans to schedule a Full System Scan. However, you should always keep Idle Time Scans turned on to allow Norton Internet Security to scan your computer when it becomes idle.

Turning off or turning on Idle Time Scans

The **Idle Time Scans** option is automatically turned on when you install Norton Internet Security. When the **Idle Time Scans** option is turned on, Norton Internet Security detects the time when you do not use your computer. Norton Internet Security then intelligently runs a scan, depending on the scan history of your computer. However, there may be times when you want to turn off **Idle Time Scans**.

To turn off Idle Time Scans

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Computer Scan**.
3. In the **Idle Time Scans** row, in the drop-down list, select **Off**.
4. Click **Apply**.

To turn on Idle Time Scans

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Computer Scan**.

3 In the **Idle Time Scans** row, in the drop-down list, select the option that you want to set. Your options are:
   - **Weekly**
   - **Monthly**
   - **Quarterly**
4 Click **Apply**.

Specifying Idle Time Out duration

You can set the duration after which Norton Internet Security should identify your computer as idle. You can select a value (in minutes) between 1 minute and 30 minutes. When you do not use your computer for the duration that you specify, Norton Internet Security checks for other predefined parameters and runs Idle Time Scans.

After you specify the **Idle Time Out** duration, you can view the **Idle Countdown** bar in the **Norton Tasks** window. The **Idle Countdown** bar displays the idle state of your computer.

To specify Idle Time Out duration from the Settings window

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **General** tab.
3 In the **Idle Time Out** row, in the drop-down list, select the duration that you want to specify. You might need to scroll the window to view the option.
4 In the **Settings** window, click **Apply**.

To specify Idle Time Out duration from the Norton Tasks window

1 In the Norton Internet Security main window, click **Performance**.
2 In the **Performance** window, click **Norton Tasks**.

3 In the **Norton Tasks** window, in the **Idle Timeout** drop-down list, select the duration that you want to specify.
4 Click **Close**.

About SONAR Protection

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. SONAR identifies threats quicker than the traditional signature-based threat detection techniques. SONAR detects and protects you against malicious code even before virus definitions are available through LiveUpdate.

SONAR monitors your computer for malicious activities through heuristic detections.

SONAR automatically blocks and removes high-certainty threats. Norton Internet Security notifies you when high-certainty threats are detected and removed. SONAR provides you the greatest control when low-certainty threats are detected. You can also suppress the SONAR notifications by disabling the **Show SONAR Block Notifications** option.

The **View Details** link in the notification alert lets you view the summary of the resolved high-certainty threats. You can also view the details under **Resolved Security Risks category** in the **Security History** window.

Turning off or turning on SONAR Protection

SONAR protects you against malicious code even before virus definitions are available through LiveUpdate. By default, SONAR Protection is turned on to proactively detect unknown security risks on your computer.

When you turn off SONAR Protection, you are prompted with a protection alert. This protection alert

lets you specify the amount of time for which you want SONAR Protection to be turned off.

When Auto-Protect is turned off, SONAR Protection is also disabled. In this case, your computer is not protected against emerging threats.

To turn off or turn on SONAR Protection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Real Time Protection**.
3. In the **SONAR Protection** row, do one of the following:
   - To turn off SONAR Protection, move the **On/Off** switch to the right to the Off position.
   - To turn on SONAR Protection, move the **On/Off** switch to the left to the On position.
4. In the **Settings** window, click **Apply**.

About Real Time Exclusions

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. SONAR identifies threats quickly compared to the traditional signature-based threat detection techniques. SONAR detects and protects you from malicious programs even before virus definitions are available through LiveUpdate.

SONAR monitors your computer for malicious activities using heuristic detections. It automatically blocks and removes high-certainty threats. Norton Internet Security notifies you when high-certainty threats are detected and removed.

However, you can configure Norton Internet Security to exclude certain programs from the Norton Internet Security Auto-Protect scans and SONAR scans. You

should exclude programs only if you are confident that they are not infected. You can exclude the programs from the Auto-Protect scans and SONAR scans by adding them to the **Real Time Exclusions** window. When you add a program to the **Real Time Exclusions** window, Norton Internet Security ignores the file when it performs Auto-Protect scan and SONAR scan. This option also excludes subfolders within a folder.

Exclude a program from Norton Internet Security scans only if you are confident that the program is safe. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer.

To add programs to the **Real Time Exclusions** window, go to the Norton Internet Security main window, and then click **Settings > Computer > AntiVirus and SONAR Exclusions > Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection > Configure**.

Excluding security threats from scanning

You can use **Scan Exclusions** window and **Real Time Exclusions** window to exclude viruses and other high-risk security threats from scanning.

To exclude high-risk security threats from scanning

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **AntiVirus and SONAR Exclusions**.
3. Do one of the following:
   - In the **Items to Exclude from Scans** row, click **Configure**.
   - In the **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection** row, click **Configure**.
4. In the window that appears, click **Add**.
5. In the **Add Item** dialog box, click the browse icon.

6 In the dialog box that appears, select the item that you want to exclude from the scan.
7 Click **OK**.
8 In the **Add Item** dialog box, click **OK**.
9 In the window that appears, click **Apply**, and then click **OK**.

About Signature Exclusions

Norton Internet Security lets you select specific known security risks and exclude them from Norton Internet Security scans. Exclude a risk from Norton Internet Security scans only if you have a specific need. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer. You might also decide not to be notified about the program in future scans.

When you exclude a known security risk from Norton Internet Security scans, the protection level of your computer reduces. You should exclude items only if you are confident that they are not infected.

To exclude a security risk from scans, you need to add the specific security risk to the **Signature Exclusions** window. The **Signature Exclusions** window contains the list of all security risks that can be excluded from Norton Internet Security scans. For each security risk, you can view the risk details and the effect of the risk on your computer.

To add security risks to the **Signature Exclusions** window, go to the Norton Internet Security main window, and then click **Settings > Computer > AntiVirus and SONAR Exclusions > Signatures to Exclude from All Detections > Configure**.

Adding items to the Signature Exclusions

To exclude a security risk from scans, you must add the specific security risk to the **Signature Exclusions** window. You can select a known risk by name and add it to the list.

When you exclude a known security risk from Norton Internet Security scans, the protection level of your computer reduces. You should exclude items only if you are confident that they are not infected.

To add a signature to the Signature Exclusions

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **AntiVirus and SONAR Exclusions**.
3. In the **Signatures to Exclude from All Detections** row, click **Configure**.
4. In the **Signature Exclusions** window, click **Add**.
5. In the **Security Risks** window, click on a security risk that you want to exclude and then click **Add**.
6. In the **Signature Exclusions** window, click **Apply**, and then click **OK**.
7. In the **Settings** window, click **OK**.

About scanning Office documents

Norton Internet Security protects all Office documents that you receive through email messages, through Internet download, and through inserted floppy disks or other removable media. By automatically scanning all Office files, Norton Internet Security maintains a higher level of security. Norton Internet Security scans the Office document when you open them.

You can use the **Microsoft Office Automatic Scan** option in the **Settings** window to scan documents of the following Microsoft Office applications:

winword.exe	Microsoft Word
excel.exe	Microsoft Excel
powerpnt.exe	Microsoft PowerPoint

visio.exe	Microsoft Visio
msaccess.exe	Microsoft Access
winproj.exe	Microsoft Project

Norton Internet Security scans the Office documents and protect against threats, including virus macros and infected embedded objects.

By default, the **Microsoft Office Automatic Scan** option in the **Settings** window is turned off. Turn on this option to scan Microsoft Office files automatically.

Turning on or turning off Microsoft Office Automatic Scan

Norton Internet Security maintains a higher level of security by automatically scanning all Office files. You can turn on the **Microsoft Office Automatic Scan** option to protect your computer against the virus macros and embedded objects.

To Turn on or turn off Microsoft Office Automatic Scan

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Computer Scan**.
3. In the **Microsoft Office Automatic Scan** row, do one of the following:
   - To turn on Microsoft Office Automatic Scan, move the **On/Off** switch to the left to the **On** position.
   - To turn off Microsoft Office Automatic Scan, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**, and then click **OK**.

About Silent Mode

Norton Internet Security provides many solutions and features to handle viruses and other security threats. Norton Internet Security displays alerts and notifications to inform you how viruses and other security threats are detected and resolved. When you perform important tasks on your computer, you likely prefer not to receive any alert messages. Norton Internet Security suppresses alerts and notifications and temporarily suspends most of the background activities based on the type of Silent Mode that is turned on.

Norton Internet Security has following types of Silent Mode:

Silent Mode	The Silent Mode that you manually turn on for a specified duration.
Full Screen Detection	The Silent Mode that Norton Internet Security turns on automatically when it detects a full-screen application and turns off when you stop using the full-screen application.

Quiet Mode	The Silent Mode that Norton Internet Security turns on automatically when it detects a disk burning task or a Media Center TV recording task. Norton Internet Security also turns on Quiet Mode automatically when you run a program that you included in the **Quiet Mode Programs** list. Norton Internet Security turns off Quiet Mode when the disk burning session or TV program recording session is complete. Norton Internet Security also turns off Quiet Mode when it stops detecting running instances of the programs that you included in the **Quiet Mode Programs** list.

The Norton Internet Security icon displays the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. The icon changes to a crescent-patterned icon when Silent Mode is turned on. Norton Internet Security also notifies you after Silent Mode is turned off.

You can view the summary of the Silent Mode sessions under the **Recent History**, **Full History**, and **Silent Mode** categories in the **Security History** window.

The summary includes the following information:

- The turn-on or turn-off status of Silent Mode
- The type of Silent Mode, such as Silent Mode or Quiet Mode
- The type of program that turns on Silent Mode, such as disk burning or TV recording
- The name of a user-specified program that turns on Silent Mode
- The time and date when Silent Mode is turned on or turned off

About the Silent Mode that you turn on manually

Norton Internet Security lets you manually turn on Silent Mode for a specified duration. When Silent Mode is turned on, Norton Internet Security suppresses alerts and suspends background activities for the duration that you specify. You can verify the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. The Norton Internet Security icon in the notification area changes to a crescent-patterned icon to display the turn-on status of Silent Mode. Turning on Silent Mode manually before you perform your tasks helps you prevent alerts, notifications, or background activities interrupting you for the specified duration.

You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. After the specified duration, Norton Internet Security turns off Silent Mode. You can also manually turn off Silent Mode at any time. Norton Internet Security notifies you after Silent Mode is turned off. The activities that are suspended when Silent Mode is turned on, run after Silent Mode is turned off.

Turning on or turning off Silent Mode manually

You can manually turn on Silent Mode for a specified duration before you perform any important task on your computer. You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. The Norton Internet Security icon displays the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. Norton Internet Security notifies you after Silent Mode is turned off. After Silent Mode is turned off, Norton Internet Security also displays alerts if it detected any security activities that occurred during the Silent Mode session.

You can turn on or turn off Silent Mode from the **Silent Mode Settings** section of the **Settings** window or from the **Norton Tasks** window. You can also turn on or turn off Silent Mode by using the Norton Internet Security icon in the notification area.

To turn on Silent Mode from the Settings window

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. In the **Silent Mode** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.
7. In the **Settings** window, click **OK**.

To turn off Silent Mode from the Settings window

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. In the **Silent Mode** row, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

To turn on Silent Mode from the Norton Tasks window

1. In the Norton Internet Security main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.
3. In the **Norton Tasks** window, under **Silent Mode**, move the **On/Off** switch to the left to the **On** position.
4. In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.
5. In the **Norton Tasks** window, click **Close**.

To turn off Silent Mode from the Norton Tasks window

1. In the Norton Internet Security main window, click **Performance**.

2 In the **Performance** window, click **Norton Tasks**.
3 In the **Norton Tasks** window, under **Silent Mode**, move the **On/Off** switch to the right to the **Off** position.
4 In the **Norton Tasks** window, click **Close**.

To turn on Silent Mode from the notification area

1 In the notification area on the Windows taskbar, right-click the Norton Internet Security icon, and then click **Turn on Silent Mode**.
2 In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.

To turn off Silent Mode from the notification area

❖ In the notification area on the Windows taskbar, right-click the Norton Internet Security icon, and then click **Turn off Silent Mode**.

About the Silent Mode that turns on automatically

When you watch a movie, play games, or make a presentation, you run the application in the full-screen mode. Norton Internet Security detects the application that you run in the full-screen mode and automatically enables Silent Mode. When Silent Mode is enabled, Norton Internet Security suppresses most of the alerts and suspends background activities. Only those activities run that are involved in protecting your computer from viruses and other security threats. Minimum background activities also ensure high performance of your computer. The activities that are suspended run after you finish using the application in the full-screen mode.

Silent Mode also helps you maintain an uninterrupted Media Center Extender session. A Media Center Extender session is an extended session of Media Center to an entertainment device, such as a television. The alerts and notifications that appear during a Media Center Extender session disconnect the session between the host computer and the entertainment device.

Norton Internet Security identifies a Media Center Extender session as an active full-screen application and turns on Silent Mode. When Silent Mode is enabled, Norton Internet Security suppresses alerts and notifications and suspends background activities to provide an uninterrupted Media Center Extender session.

Turning off or turning on Full Screen Detection

You can use the **Full Screen Detection** option in the **Settings** window to turn on or turn off Silent Mode automatically when Norton Internet Security detects a full-screen application. By default, the **Full Screen Detection** option remains turned on after you install Norton Internet Security.

To turn off Full Screen Detection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. In the **Full Screen Detection** row, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

To turn on Full Screen Detection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. In the **Full Screen Detection** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

About Quiet Mode

Norton Internet Security automatically enables Quiet Mode when you perform a few tasks that require higher utilization of your system resources. When Quiet Mode is turned on, Norton Internet Security suspends the background activities and lets the task use the maximum resources for better performance.

You can choose to set Norton Internet Security to automatically enable Quiet Mode when you do the following tasks:

- IMAPI 2.0 Disk Burn
- Media Center TV Recording
- User-Specified Programs

In addition, you can configure Norton Internet Security to enable Quiet Mode when you run a program of your choice.

The following table explains about the various options:

IMAPI 2.0 Disk Burn	When you use a Media Center application to burn a CD or a DVD, Norton Internet Security automatically enables Quiet Mode, if the **IMAPI 2.0 Disk Burn** option is turned on. By default, the **IMAPI 2.0 Disk Burn** option is turned on. When Quiet Mode is enabled, Norton Internet Security suspends background activities to improve the performance of your disk-burning session. However, Norton Internet Security continues to display alerts and notifications during the session. Norton Internet Security supports the following Media Center disk-burner applications to turn on Quiet Mode: ▪ IMAPI 2.0 ▪ J. River MEDIA CENTER (version 13.0.125 and later) Norton Internet Security turns on Quiet Mode as soon as you start burning a CD or a DVD using a Media Center application. Norton Internet Security turns off Quiet Mode after the disk-burning session is complete. You cannot turn off Quiet Mode during the disk-burning session by turning off the **IMAPI 2.0 Disk Burn** option in the **Settings** window.

Media Center TV Recording	When you use a Media Center application to record a TV program, Norton Internet Security automatically enables Quiet Mode, if the **Media Center TV Recording** option is turned on. By default, the **Media Center TV Recording** option is turned on. When Quiet Mode is enabled, Norton Internet Security suspends background activities to improve the performance of your TV program recording session. However, Norton Internet Security continues to display alerts and notifications during the session. Norton Internet Security supports the following Media Center applications to turn on Quiet Mode: ▪ Windows Media Center For Windows Media Center to enable Quiet Mode during TV program session, you might need to restart your computer after you install Norton Internet Security. ▪ J. River MEDIA CENTER (version 13.0.125 and later) Norton Internet Security turns on Quiet Mode as soon as you start recording a TV program. After Quiet Mode is turned on, it turns off after the recording session is complete. You cannot turn off Quiet Mode during the TV program recording session by turning off the **Media Center TV Recording** option in the **Settings** window.

User-Specified Programs	Norton Internet Security automatically turns on Quiet Mode when it detects a TV program recording session or a disk-burning session. In addition, you can manually add the programs for which you want Norton Internet Security to turn on Quiet Mode to the **Quiet Mode Programs** list. When Norton Internet Security detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton Internet Security suspends the background activities but does not suppress alerts and notifications. You can also add or remove a running program to the **Quiet Mode Programs** list.

Turning off or turning on the Quiet Mode options

You can turn off or turn on the Quiet Mode options, such as **IMAPI 2.0 Disk Burn** or **Media Center TV Recording** in the **Settings** window. By default, the Quiet Mode options are turned on. If you perform a task for an option that you turned on, Norton Internet Security detects the task and automatically turns on Silent Mode. For example, you turn on the **IMAPI 2.0 Disk Burn** option and start burning a disk using a Media Center application. In this case, Norton Internet Security detects the disk-burning session and turns on Quiet Mode.

Norton Internet Security turns on Quiet Mode as soon as you start recording a TV program or burning a CD or a DVD. Once Quiet Mode is turned on, it turns off

only after the TV program recording session or disk-burning session is complete. You cannot turn off Quiet Mode during the sessions by using the options in the **Settings** window.

To turn off or turn on IMAPI 2.0 Disk Burn

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. Under **Quiet Mode on Detection of:**, do one of the following:
   - To turn off detection of a disk burning session, in the **IMAPI 2.0 Disk Burn** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on detection of a disk burning session, in the **IMAPI 2.0 Disk Burn** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

To turn off or turn on Media Center TV Recording

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. Under **Quiet Mode on Detection of:**, do one of the following:
   - To turn off detection of a TV program recording session, in the **Media Center TV Recording** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on detection of a TV program recording session, in the **Media Center TV Recording** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

About User-Specified Programs

Norton Internet Security automatically turns on Quiet Mode when it detects a TV program recording session or a disk-burning session. In addition, you can manually add the programs for which you want Norton Internet Security to turn on Quiet Mode to the Quiet Mode Programs list. When Norton Internet Security detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton Internet Security suspends the background activities but does not suppress alerts and notifications.

You can also add a running program to the Quiet Mode Programs list. However, when you add a running program, Norton Internet Security does not detect the current running instance of the program to turn on Quiet Mode. Norton Internet Security turns on Quiet Mode the next time when you execute the program.

You can also remove a running program from the Quiet Mode Programs list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

You can view the details of the programs that you add to the Quiet Mode Programs list or remove from the list in the **Security History** window.

Adding programs to User-Specified Programs

You can manually add the programs for which you want Norton Internet Security to turn on Quiet Mode to the Quiet Mode Programs list. When you execute the program that you added to the list, Norton Internet Security detects the program and turns on Quiet Mode.

You can also add a running program to the **Quiet Mode Programs** list. However, when you add a running program, Norton Internet Security does not detect the current running instance of the program to turn on

Quiet Mode. Norton Internet Security turns on Quiet Mode the next time when you execute the program.

You can only add the programs that have .exe file extension to the **Quiet Mode Programs** list.

To add a program

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.
4. Under **Quiet Mode on Detection of**, in the **User-Specified Programs** row, click **Configure**.
5. In the **Quiet Mode Programs** window, click **Add**.
6. In the **Add Program** dialog box, navigate to the location of the file that you want to add to the Quiet Mode Programs list.
7. Select the file, and then click **Open**.
8. Click **Apply**.
9. In the **Quiet Mode Programs** window, click **OK**.

Removing programs from User-Specified Programs

You can remove a program from the **Quiet Mode Programs** list. After you remove a program, Norton Internet Security does not turn on Quiet Mode the next time when it detects a running instance of the program.

You can also remove a running program from the **Quiet Mode Programs** list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

To remove a program

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Silent Mode Settings**.

4 Under **Quiet Mode on Detection of**, in the **User-Specified Programs** row, click **Configure**.
5 In the **Quiet Mode Programs** window, select the program that you want to delete, and then click **Remove**.
6 In the confirmation dialog box, click **Yes**.
7 In the **Quiet Mode Programs** window, click **OK**.

About boot time protection

The boot time protection feature provides enhanced security level from the time you start your computer. It ensures better security by running all the necessary components that are required for computer protection as soon as you start your computer.

To protect your computer during boot time, you must configure the **Enable Boot Time Protection** option. To access the **Enable Boot Time Protection** option, go to the Norton Internet Security main window, and then click **Settings > Computer > Real Time Protection**.

You can use the following options to configure **Enable Boot Time Protection**:

- **Aggressive**

  Provides maximum protection during your computer start time.

  This option ensures complete protection during the boot time as Auto-Protect starts functioning as soon as you start your computer.

- **Normal**

  Provides enhanced protection during your computer start time without compromising your computer's boot performance.

  When you select this option, the drivers and plug-ins start functioning during the computer start time before their specified time delay. This option ensures better boot performance along with good security levels.

- **Off**

Turns off boot time protection.

If you turn off the **Enable Boot Time Protection** option, the protection level of your computer reduces.

Configuring boot time protection

The boot time protection feature provides enhanced security level from the time you start your computer. As soon as you start your computer, Norton Internet Security starts Auto-Protect and all required drivers and plug-ins start functioning. This feature ensures higher level of security from the moment you turn on your computer.

To configure boot time protection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Real Time Protection**.
3. In the **Enable Boot Time Protection** row, click on one of the settings. Your options are:
   - **Aggressive**
   - **Normal**
   - **Off**
4. Click **Apply**, and then click **OK**.

Responding to security issues

4

This chapter includes the following topics:

- What to do if a security risk is found

What to do if a security risk is found

Your product provides many solutions and features for handling viruses and other security threats that it detects.

When Norton Internet Security detects a security risk on your computer, you must take appropriate action on the risk. Norton Internet Security notifies you when it detects a security risk. You can view details about the risk in the window that appears and select an action that you want Norton Internet Security to perform on the risk.

By default, Norton Internet Security removes the security risk from your computer and quarantines it. However, you can restore the file from the Quarantine to its original location and exclude it from future scans.

Exclude a program from Norton Internet Security scans only if you are confident that the program is safe. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer.

In some cases, Norton Internet Security requires your attention to manually resolve the detected security

risk. You can access the Symantec Security Response Web site and refer the manual removal instructions.

In some cases, Norton Internet Security might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can submit the item to Symantec for further analysis.

In addition, your product provides solutions for security risks, such as spyware and adware.

About detecting viruses, spyware, and other risks

Viruses and other security threats can be detected during a manual or scheduled scan. Auto-Protect detects these threats when you perform an action with an infected file. Threats can also appear during an instant messenger session, when you send an email message, or during a manual or scheduled scan.

Security risks, such as spyware and adware, can also be detected when these activities are performed.

The files that can potentially infect your system when your computer first starts up are scanned first.

These files include the following:

- Files that are associated with the processes that are currently running in memory
- Files with startup folder entries
- Files with system start INI file entries
- Files with system start batch file entries
- Files that the system start registry keys refers

If an infected file is detected during this portion of the manual scan, it is repaired or removed. Any unnecessary references are also removed from your computer. Before attempting to repair, quarantine, or delete any infected file that has a process running in memory, your product attempts to terminate the process. You are alerted and prompted to close all unnecessary programs before the process is terminated.

You can view information about detected viruses and other security threats in Security History.

Security History also includes information about spyware, adware, and other security risks.

Reviewing Auto-Protect notifications

Auto-Protect scans files for viruses, worms, and Trojan horses when you perform an action with them, such as moving them, copying them, or opening them.

It also scans for spyware, adware, and other security risks.

If Auto-Protect detects suspicious activity, it logs a notification in Security History that tells you that a risk was found and resolved.

If Auto-Protect detect one or more viruses it either repairs or deletes the viruses and notifies you. The notification provides information on which file was repaired or deleted and which virus, Trojan horse, or worm infected the file. No further action is necessary.

To review Auto-Protect notifications

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **History**.

3 In the **Show** drop-down list, select the category for which you want to review Auto-Protect alerts. Your options are:

Recent History	Review Auto-Protect notifications that you received in the last seven days.
Full History	Review all of the Auto-Protect notifications that you have received.
Resolved Security Risks	Review all of the resolved security threats. The **Resolved Security Risks** category includes the infected files that Norton Internet Security repairs, removes, or quarantines.
Unresolved Security Risks	Review the list of unresolved security risks. The **Unresolved Security Risks** category includes the infected files for which Norton Internet Security was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action.

4 In the right pane, click the **Options** link.
The option name appears as **Restore & Options** for few items.
If one or more security risks such as spyware are found, you can take action on these items, if required.

5 In the **Threat Detected** window, select the appropriate action on the risk.
The following are some of the options that are available in the **Threat Detected** window:

Restore & Exclude this file	Returns the selected Quarantine item to its original location and excludes the item from being detected in the future scans. This option is available for the detected viral and non-viral threats.
Exclude this program	Excludes the security risk from future scan. Norton Internet Security adds the security risk to the appropriate exclusions list.
Remove this file (may cause browser to close) (recommended)	Removes the security risk from your computer and quarantines it. This option is available for the security risks that require your attention.

Remove this file (may cause browser to close)	Removes the selected security risk from the computer and quarantines it. This option is available for the security risks that require your attention for manual removal. This option is also available for the security risks that are manually quarantined.
Remove from history	Removes the selected security risk item from the Security History log.
Get help (recommended)	Takes you to the Symantec Security Response Web site. This option is available for the security risks that require your attention for manual removal. You can refer the Symantec Security Response Web site for manual removal instructions or other information about the risk.

Submit to Symantec	Sends the security risk to Symantec. In some cases, Norton Internet Security might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can use this option to submit the item to Symantec for further analysis.

Responding to Worm Blocking alerts

If a program tries to email itself or a copy of itself, it could be a worm trying to spread through email. A worm can send itself or send a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for worms. If it detects a worm, you receive an alert notifying you that a malicious worm was found.

Worm Blocking alert appears only when you enable the **Ask me what to do** option under **How to respond when an outbound threat is found** in the **Email Antivirus Scan** window. If the **Ask me what to do** option is disabled Norton Internet Security automatically quarantines the detected worm and notifies you.

The alert presents you with options and asks you what to do. If you do not send an email message at that time, then it is probably a worm and you should quarantine the file.

To respond to Worm Blocking alerts

❖ In the alert window, select the action that you want to take. Your options are:

Quarantine	Permanently stops the worm by putting it in Security History. While in Security History, the worm is unable to spread. This Quarantine is the safest action.
Allow	Sends the email message for which you have received the worm blocking alert. If you allow the email message, it could infect the recipient's computer. Select this option if you are sure that the email is not infected with a worm.
Ignore	Ignores this risk.

If a malicious worm is found, it should be quarantined.

To quarantine a worm-infected file

1 In the alert, in the drop-down list, click **Quarantine**.

2 After the worm has been quarantined, perform the following tasks:

- Run LiveUpdate to ensure that you have the latest definition updates.

  See "About Program and Definition Updates" on page 50.
- Scan your computer.

  See "Running a Full System Scan" on page 118.

If nothing is detected, submit the infected file to Symantec Security Response. Also, indicate that the file was detected and that you have scanned it with the latest definition updates. Symantec Security Response replies to you within 48 hours.

About responding to risks detected during a scan

At the end of a scan, the **Results Summary** window provides the summary of the scan results. You can use the **Threats Detected** window to resolve any items that were not automatically resolved during the scan.

The **Recommended Action** section in the **Security History** window displays the action that you should take to resolve the security threat.

About actions when Norton Internet Security cannot repair a file

One of the common reasons that Norton Internet Security cannot automatically repair or delete an infected file is that you do not have the current definition updates. Run LiveUpdate, and then scan again.

Before running LiveUpdate to receive protection updates, ensure that Quick Scan is turned on (it is turned on by default). After LiveUpdate retrieves the latest definition updates, Quick Scan automatically checks for the infections that have processes running in memory. It also checks for the infections that the start-up files and folders refer.

If that does not work, read the information on the **Threats Detected** window to identify the types of files

that cannot be repaired. You can take one of the following actions, depending on the file type:

Infected files	

	You can view the file type of the detected risk. This information helps you to decide the action that can be taken depending on the file type. For example, you can view the infected files with the following file name extensions (any file can be infected): ▪ .exe ▪ .doc ▪ .dot ▪ .xls Use the **Threats Detected** window to solve the problem.

Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using your operating system disks.

Resolving a suspected security risk

Norton Internet Security needs to close a suspected security risk program to resolve it.

To resolve the suspected security risk

- Save all open files, and then click **Go**.
  If you do not respond to this dialog box, it closes automatically without resolving and closing the suspected security risk.

Protecting Internet activities

5

This chapter includes the following topics:

- About the Smart Firewall
- About Download Insight
- About Intrusion Prevention
- About Vulnerability Protection
- About the types of security risks
- About Norton AntiSpam
- About configuring POP3 and SMTP ports
- About the Network Security Map
- About Metered Broadband Mode

About the Smart Firewall

The Smart Firewall monitors the communications between your computer and other computers on the

Internet. It also protects your computer from such common security problems as the following:

Improper connection attempts	Warns you of connection attempts from other computers and of attempts by programs on your computer to connect to other computers
Port scans	Cloaks the inactive ports on your computer thereby providing protection against attacks through hacking techniques such as port scanning
Intrusions	Monitors the network traffic to or from your computer for suspicious behavior and stops any attack before they threaten your system

A firewall blocks hackers and other unauthorized traffic, while it allows authorized traffic to pass. Turning off Smart Firewall reduces your system protection. Always ensure that the Smart Firewall is turned on.

About firewall rules

A firewall is a security system that uses rules to block or allow connections and data transmission between your computer and the Internet. Firewall rules control how the Smart Firewall protects your computer from malicious programs and unauthorized access. The firewall automatically checks all traffic that comes in or out of your computer against these rules.

The Smart Firewall uses two kinds of firewall rules:

Program rules	Control network access for programs on your computer.
General rules	Control all the incoming and the outgoing network traffic.

About the order in which firewall rules are processed

The Smart Firewall processes General rules before it processes Program rules. For example, consider a case when there is a Program rule that allows Internet Explorer to access Internet using port 80 with TCP protocol and a General rule that blocks TCP communication through port 80 for all applications. In this case, the Internet Explorer application cannot access the Internet as Norton Internet Security gives precedence to General rules over the Program rules.

Within the list of General rules, rules are processed in order of appearance, from top to bottom. **Program Control** entries are not processed in order. The rules within each **Program Control** entry, however, are processed in order of appearance, from top to bottom.

For example, you have a Program rule for the Symantec pcAnywhere application that blocks the use of the application with any other computer. You add another rule for the same application that allows its use with a specific computer. You then move the new rule before the original rule in the program rule list. Norton Internet Security processes the new rule first and lets you use Symantec pcAnywhere with that specific computer. It then processes the original rule and prevents its use with any other computer.

About General rules

Norton Internet Security includes a number of predefined general firewall rules. These rules provide

network functionality and protection from known Internet risks. Examples of default firewall rules include the following:

Default Allow Specific Inbound ICMP Default Allow Specific Outbound ICMP	Permit all types of outbound and safe types of inbound ICMP (Internet Control Message Protocol) messaging. ICMP messages provide status and control information.
Default Allow Inbound NetBIOS Name (Shared Networks) Default Allow Inbound NetBIOS (Shared Networks)	Permit the use of the NetBIOS name service and the NetBIOS datagram service that the Microsoft Network uses in file and printer sharing.
Default Allow Inbound Bootp Default Allow Outbound Bootp	Permit the use of the Bootp service. Bootp is short for Bootstrap Protocol, which enables a computer to discover its own IP address.

The **General Rules** window displays a list of predefined general rules. These rules appear in the order of their priority levels. Rules that appear higher in the list override the rules that appear lower in the list.

You can add a new General rule in this window. You can also do the following activities:

Modify a General rule	You can change the settings of a General rule that does not function the way you want. However, you cannot modify some of the default rules that are locked. See "Modifying General rules and Program rules" on page 212.
Turn off a General rule	You can disable a General rule. However, you cannot turn off some of the default rules that are locked. See "Turning off a General rule temporarily" on page 215.
Change the priority of a General rule	You can change the priority of a General rule by changing where it appears in the list. Only advanced users or novice users at the direction of technical support, should perform this action. See "Changing the order of firewall rules" on page 214.

About Program rules

Program rules control network access for the programs that are on your computer. You can use the Program Control feature to create and modify rules for programs.

The **Program Control** window displays a list of programs. In this window, you can do the following:

- Add a program.
- Rename a program.
- Modify the rules for a program.
- Add a rule for a program.
- Modify the access settings of a program rule.
- Modify the priority of a program rule by changing the sequence of rules in the list.
- Remove a program rule.
- Remove a program.

You can create Program rules in the following ways:

Automatically customize Internet access settings	Lets the firewall automatically configure access for programs the first time that users run them. This method is the easiest way to create firewall rules.
Use Program Control	Manages the list of programs that can access the Internet.

Respond to alerts	Lets the firewall notify you when a program attempts to access the Internet. You can then allow or block Internet access for the program. In some instances, such as when you watch a movie, you might prefer not to be alerted with any messages. In such cases, you can turn on Automatic Program Control. Norton Internet Security does not prompt you with any firewall alerts in this state. The firewall notifies you only if you have changed the **Advanced Settings** options of Smart Firewall from their default, recommended settings.

Turning off Automatic Program Control

Automatic Program Control automatically configures Internet access settings for Web-enabled programs the first time that they run. When a program tries to access the Internet for the first time, Automatic Program Control creates rules for it.

Automatic Program Control configures Internet access only for the versions of programs that Symantec recognizes as safe. An alert occurs when an infected program tries to access your computer.

If you want to determine the Internet access settings for your programs, you can turn off Automatic Program Control. When a program tries to access the Internet

for the first time, an alert prompts you to configure access settings.

When you turn off Automatic Program Control, a warning appears. Symantec recommends that Automatic Program Control remain turned on. By turning it off, you might make the incorrect decisions that can allow malicious programs to run or block critical Internet programs and functions.

After you turn off Automatic Program Control, you can turn on the Advanced Events Monitoring feature.

When you turn on any Advanced Events Monitoring feature, you are prompted with numerous firewall alerts that prompt you to allow or deny network access for any unrecognized program the first time that it runs or that is not currently handled by the firewall rules or the Advanced Events Monitoring feature.

When you turn on Automatic Program Control, the Advanced Events Monitoring features are disabled. The **Advanced Events Monitoring** settings that you configured are no longer applicable.

To turn off Automatic Program Control

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Firewall**.
4. Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.
5. In the **Advanced Settings** window, in the **Automatic Program Control** row, move the **On/Off** switch to the right to the **Off** position.
6. In the window that appears, click **Yes**.
7. In the **Advanced Settings** window, click **Apply**, and then click **OK**.

Adding a program to Program Control

You can add a program to Program Control to control their ability to access the Internet. When you add the

program, you can configure its access settings in Program Control. You can allow, block, or create the custom rules that are specific to the program that you add.

Manually configured Firewall settings for programs override any settings that Automatic Program Control makes. However, Symantec recommends you to retain the settings that Automatic Program Control makes as and when you run your programs.

To add a program to Program Control

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Firewall**.
4. Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
5. In the **Program Control** window, click **Add**.
6. In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
7. Click **Open**.

8 In the **Security Request - Program Control** window, in the **What do you want to do?** drop-down list, select the access level that you want this program to have. Your options are:

Allow	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet access (Recommended)	Create the rules that control how this program accesses the Internet. You can set the following criteria for a rule: ■ **Action** ■ **Connections** ■ **Computers** ■ **Communications** ■ **Advanced** ■ **Description** If you select this option, you must follow the instructions in the wizard that appears and configure the rule.

9 Click **OK**.

Removing a program from Program Control

You can remove programs from Program Control if necessary. In this case, Norton Internet Security removes all the rules that are associated with the application that you remove.

The firewall settings for the programs are not migrated from previous versions of Norton Internet Security. If

you removed any programs in the previous version and do not want them in the current version, you must remove them again.

To remove a program from Program Control

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
4. In the **Program Control** window, in the **Program** column, select the program that you want to remove.
5. Click **Remove**.
6. In the **Confirmation** dialog box, click **Yes**.
   The confirmation dialog box appears only when the **Automatic Program Control** option is turned off.
7. Click **OK**.

Customizing Program Control

After you use Norton Internet Security for a while, you might need to change the access settings for certain programs.

To customize Program Control

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Smart Firewall**.
4. Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
5. In the **Program Control** window, in the **Program** column, select the program that you want to change.

6 In the drop-down list next to the program that you want to change, select the access level that you want this program to have. Your options are:

Allow	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Custom	Create the rules that control how this program accesses the Internet.

The **Auto** option is the default option that is assigned automatically to a program when Automatic Program Control is turned on.

7 Click **OK**.

Adding General rules and Program rules

Program Control automatically creates most of the firewall rules that you need. You can add custom rules if necessary.

Only experienced users should create their own firewall rules.

You can add the following types of firewall rules:

- General rules
- Program rules

To add a General rule

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.

5 In the **Advanced Settings** window, in the **General Rules** row, click **Configure**.
6 In the **General Rules** window, click **Add**.
7 Follow the instructions in the **Add Rule** wizard.
8 In the **General Rules** window, click **OK**.
9 In the **Advanced Settings** window, click **OK**.

To add a Program rule

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
5 In the **Program Control** window, in the **Program** column, select the program to which you want to add a rule.
6 Click **Modify**.
You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
7 In the **Rules** window, click **Add**.
8 Follow the instructions in the **Add Rule** wizard.
9 In the **Rules** window, click **OK**.
10 In the **Program Control** window, click **OK**.

Using the Add Rule Wizard

The **Add Rule** Wizard leads you through the steps that are necessary to create firewall rules.

To use the Add Rule Wizard

1 Open the **Add Rule Wizard** by creating a General rule or a Program rule.

2 In the first panel of the **Add Rule Wizard**, select the action that you want for this rule. Your options are:

Allow	Allow communication of this type. For example, consider a General rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Allow**, Smart Firewall allows all connections satisfying the criteria of this General rule.
Block	Prevent communication of this type. For example, consider a General rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Block**, Smart Firewall blocks all connections satisfying the criteria of this General rule.

Monitor	Update the **Firewall – Activities** category in the event log each time that communication of this type takes place. This option lets you monitor how often this firewall rule is used. Norton Internet Security notifies you every time that the traffic matching the monitor rule criteria passes through your computer. You can use the links in these notifications to view the logs. You can view the event log under **Firewall – Activities** category in the **Security History** window. Norton Internet Security creates separate action rules to allow or block the programs that have only a **Monitor** rule associated with them. The **Monitor** rule must be of higher order than the action rule for successful log entry of the network event that is related to the program.

3 Click **Next**.

4 Select the type of connection for the rule. Your options are:

Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to inbound and to outbound connections.

5 Click **Next**, and then select the computers that apply to the rule. Your options are:

Any computer	The rule applies to all computers.
Any computer in the local subnet	This rule applies only to computers in the local subnet. An organization's network is divided into subnets to facilitate efficient Internet communications. A subnet represents all of the computers in the same LAN.
Only the computers and sites listed below	The rule applies only to the computers, sites, or domains that you specify. You can specify the names and addresses of computers that apply to the rule. The details of the specified computers appear in the list. You can also remove computers from the list. When you select this option, the **Add** option becomes available. You can then specify or remove a computer by using the **Add** or the **Remove** options.

6 Click **Next**, and then select the protocols for the rule. Your options are:

TCP	The rule applies to TCP (Transmission Control Protocol) communications.
UDP	The rule applies to UDP (User Datagram Protocol) communications.
TCP and UDP	The rule applies to TCP and to UDP communications.
ICMP	The rule applies to ICMP (Internet Control Message Protocol) communications. This option is available only when you add or modify a General rule.
ICMPv6	The rule applies to ICMP (Internet Control Message Protocol for Internet Protocol version 6) communications. This option is available only when you add or modify a General rule.

All	The rule applies to all supported protocols. When you select this option, you cannot specify the types of communications or ports that apply to the rule.

7 Select the ports for the rule. Your options are:

All types of communication (all ports, local and remote)	The rule applies to communications that use any port.
Only communications that match all types and ports listed below	The rule applies to the ports that you specify. You can specify the ports by selecting from the listed ports or by adding specific ports or port ranges. If you select ICMP or ICMPv6 protocol, you can specify the commands. To do so, select a command from the list of known commands or add specific commands or command ranges. When you select this option, the **Add** option becomes available. You can use the **Add** option or the **Remove** option to specify or remove a port or a command.

8 Click **Next**.

9 Check **Create a Security History log entry** if you want Norton Internet Security to create an entry in the firewall event log.
Norton Internet Security creates an entry when a network communication event matches this rule. You can view the event log in the **Security History** window under **Firewall – Activities**. If you selected the **Monitor** option in the **Action** window, then the **Create a Security History log entry** option is automatically checked. You cannot uncheck the box to turn off this option as it is the default setting.

10 Check **Apply this rule** if you want to apply this rule to Ipv6 NAT Traversal traffic.

11 Click **Next**, and then, in the text box, type a name for this rule.

12 Click **Next**, and then review the new rule settings.

13 Click **Finish**.

14 When you have finished adding rules, click **OK**.

Modifying General rules and Program rules

You can change an existing firewall rule if it does not function the way that you want. You can use the **Modify** option to change the settings of an existing firewall rule. When you change a rule, the firewall uses the new criteria of the modified rule to control network traffic.

You cannot modify some of the default rules that are locked. However, you can view the settings of these rules by using the **View** option.

To modify a General rule

1 In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Network** tab.

3 In the left pane, click **Smart Firewall**.

4 Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.

5 In the **Advanced Settings** window, in the **General Rules** row, click **Configure**.
6 In the **General Rules** window, select the rule that you want to change.
7 Click **Modify**.
8 In the **Modify Rule** window, make the necessary changes to modify any aspect of the rule.
9 When you have finished changing the rule, click **OK**.
10 In the **General Rules** window, click **OK**.
11 In the **Advanced Settings** window, click **OK**.

To modify a Program rule

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
5 In the **Program Control** window, in the **Program** column, select the program that you want to change.
6 Click **Modify**.
You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
7 In the **Rules** window, select the rule that you want to change.
8 Click **Modify**.
9 In the **Modify Rule** window, make the necessary changes to modify to change any aspect of the rule.
10 When you have finished changing the rule, click **OK**.
11 In the **Rules** window, click **OK**.
12 In the **Program Control** window, click **OK**.

Changing the order of firewall rules

Each list of firewall rules is processed from the top down. You can adjust how the firewall rules are processed by changing their order.

Do not change the order of the default General rules unless you are an advanced user. Changing the order of default General rules can affect firewall functionality and reduce the security of your computer.

To change the order of General rules

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Smart Firewall**.
4. Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.
5. In the **Advanced Settings** window, in the **General Rules** row, click **Configure**.
6. In the **General Rules** window, select the rule that you want to move.
7. Do one of the following:
   - To move this rule before the rule above it, click **Move Up**.
   - To move this rule after the rule below it, click **Move Down**.
8. When you are done moving the rules, click **OK**.
9. In the **Advanced Settings** window, click **OK**.

To change the order of Program rules

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Smart Firewall**.
4. Under **Smart Firewall**, in the **Program Control** row, click **Configure**.

5 In the **Program Control** window, in the **Program** column, select the program that contains the rule that you want to move.
6 Click **Modify**.
7 In the **Rules** window, select the rule that you want to move.
8 Do one of the following:
   - To move this rule before the rule above it, click **Move Up**.
   - To move this rule after the rule below it, click **Move Down**.
9 When you are done moving the rules, click **OK**.
10 In the **Program Control** window, click **OK**.

Turning off a General rule temporarily

You can temporarily turn off a general rule if you need to allow specific access to a computer or a program. You must remember to turn on the rule again when you are done working with the program or computer that required the change.

You cannot turn off some of the default firewall rules that appear in the list. You can only view the settings of these rules by using the **View** option.

To turn off a General rule temporarily

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.
5 In the **Advanced Settings** window, in the **General Rules** row, click **Configure**.
6 In the **General Rules** window, uncheck the box next to the rule you want to turn off.
7 Click **OK**.
8 In the **Advanced Settings** window, click **OK**.

Removing a firewall rule

You can remove some of the firewall rules if necessary. However, you cannot remove some of the default General rules that appear in the list. You can view the settings of these rules by using the **View** option.

Do not remove a firewall rule unless you are an advanced user. Removing a firewall rule can affect firewall functionality and reduce the security of your computer.

To remove a General rule

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Smart Firewall**.
4. Under **Smart Firewall**, in the **Advanced Settings** row, click **Configure**.
5. In the **Advanced Settings** window, in the **General Rules** row, click **Configure**.
6. In the **General Rules** window, select the rule that you want to remove.
7. Click **Remove**.
8. In the **Confirmation** dialog box, click **Yes**.
9. When you are done removing rules, click **OK**.
10. In the **Advanced Settings** window, click **OK**.

To remove a Program rule

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Smart Firewall**.
4. Under **Smart Firewall**, in the **Program Control** row, click **Configure**.
5. In the **Program Control** window, in the **Program** column, select the program that contains the rule that you want to remove.

6 Click **Modify**.
To remove all the program rules that are associated with the program, click **Remove**.

7 In the **Rules** window, select the rule that you want to remove.

8 Click **Remove**.

9 In the **Confirmation** dialog box, click **Yes**.

10 When you are done removing rules, click **OK**.

11 In the **Program Control** window, click **OK**.

12 Click **OK**.

About Smart Firewall settings

The **Smart Firewall** options let you customize how the firewall monitors and responds to inbound communications and outbound communications.

You can change the Smart Firewall settings only if you have the administrator permissions.

You can set the following **Smart Firewall** options:

Advanced Settings	Control settings of the advanced protection features of Smart Firewall.
Program Control	Control settings for the programs that access the Internet.
Trust Control	View the networks that your computer is connected to, and add the networks and computers to the Trusted list or the Restricted list.

Block All Network Traffic	Lets you configure how Norton Internet Security must control the network communications to and from your computer. For instance, you may have to be away from your system for a very long time. During this period, you want to secure your system by not allowing it to communicate with the other computers on the network. In such cases, you can use the **Block All Network Traffic** option to block all the communications to and from your computer.

About Smart Firewall Program Control settings

Smart Firewall Program Control settings let you control options for the programs that access the Internet.

In the list of programs, you can modify Internet access for each program. You can also add a program to the list or remove a program from the list. Your options are:

Program	Displays the name of the program, or the name of the program's executable file

Access	Displays the level of access that the program has You can change the access level by selecting a different entry from the drop-down list. Your options are **Allow**, **Block**, and **Custom**. The **Auto** option is the default option that is assigned automatically to a program when Automatic Program Control is turned on.
Add	Lets you add a program to Program Control manually
Modify	Opens the **Rules** window, in which you can customize rules for a selected program
Remove	Lets you remove a selected program from Program Control
Rename	Lets you change the description for the selected program In this case, the file name does not change.

About Smart Firewall Trust Control settings

You can use the Smart Firewall Trust Control settings to view the devices on the network to which your computer is connected.

This feature also lets you do the following:

- Select the networks or computers you can trust at certain levels of access.

- Select the networks or computers you want to completely restrict from directly accessing your computer.

When you select **Trust Control**, the **Network Security Map** window appears. Some of the activities that you can do in this window are the following:

- View the details of the devices that are present in the network.
- Monitor the connection status of the devices that are present in the network.
- View the security status of your network connection.
- View the security status of each computer that you remotely monitor.
- View the Trust Control status of all the devices that are on your Network Security Map.

About Smart Firewall Advanced Settings

Smart Firewall Advanced Settings let you activate advanced protection features of Smart Firewall. Your options are:

General Rules	Determines how the Smart Firewall controls incoming network traffic and outgoing network traffic
Uncommon Protocols	Determines how the Smart Firewall handles uncommon protocols such as Internet Group Management Protocol (IGMP) and IPv6 Hop-by-Hop Option (HOPOPT)

Firewall Reset	

	Returns the Smart Firewall to its default state. You can click **Reset** to ensure that all recommended firewall rules and settings are configured. Norton Internet Security prompts you with a confirmation dialog box when you reset firewall. If you reset the firewall, you remove any custom rules or settings that you have configured. Resetting the firewall clears the AutoBlock computers and also changes the **Trust Control** settings in the Network Security Map. In Windows XP, Norton Internet Security prompts you to select the trust level of the network after you reset the firewall. The alert appears only if your computer matches the following criteria: ▪ You need to set the Automatic File/Printer Sharing Control to **Ask Me** ▪ Your computer must have at least one shared resource or the operating system need to be Windows Media Center edition ▪ Your computer must use a private IP

	address range ▪ Your computer must be connected to a secure wireless or wired connection
Stealth Blocked Ports	Ensures that blocked and inactive ports do not respond to connection attempts Prevents the active ports from responding to connection attempts with incorrect source or destination information.
Stateful Protocol Filter	Automatically allows the Internet traffic that matches the connections that an application opens Check this option to do the following: ▪ Analyze the network traffic that enters your computer. ▪ Block the suspicious applications that try to connect to your computer.

Automatic File/Printer Sharing Control	

	Allows the computers on the network to share resources such as files, folders, and printers (that are locally attached) Some of the Windows 7 features such as Home Media Experience work only when the trust level of the network to which your computer is connected is set to Shared or Full Trust. When Automatic File/Printer Sharing Control is turned on, it sets the trust level of the network to Shared only if certain other security criteria such as the following match: ▪ Your computer must have at least one shared resource or the operating system need to be Windows Media Center edition ▪ Your computer must use a private IP address range ▪ Your computer must be connected to a secure wireless or wired connection You can set this option to **On** or **Off** state. In windows XP, you can also set this option to **Ask Me**. In this state, Norton Internet Security prompts you before it classifies a

	new network to which your computer is connected as Shared or Protected. The prompt appears only when the security criteria for sharing matches.

Automatic Program Control	

	Automatically configures Internet access settings for the Web-enabled programs that are run for the first time The **Automatic Learn IPv6 NAT Traversal Traffic** option is available only when Automatic Program Control is turned on. Norton Internet Security provides this option to control the network traffic that uses Teredo to communicate with your computer. Some of the Windows 7 features such as Remote Media Experience and Remote Assistance work only when Automatic Learn IPv6 NAT Traversal Traffic is on. When you turn off Automatic Program Control , you can turn on Advanced Events Monitoring. You can use the **Advanced Events Monitoring** options, to configure the Internet access settings for Internet-enabled programs the first time that they run. When you turn on Advanced Events Monitoring feature, you are prompted with numerous firewall alerts. If you do not want to

	receive firewall alerts, you can turn on Automatic Program Control. The **Advanced Events Monitoring** settings consist of the following categories that provide your computer with advanced protection:

- **Program Component**

  This option protects you against the malicious programs that launch Internet-enabled programs.
- **Program Launch**

  This option protects you against the malicious programs that attach to safe programs without being detected.
- **Command Line Execution**

  This option protects you against the Trojan horses or malicious programs that launch trusted applications in hidden mode through-command line parameters.
- **Code Injection**

  This option protects you against the Trojan horses or malicious programs that inject code into an application's process without firewall alerts.
- **Window Messages**

  This option protects you against the Trojan horses and other malicious programs that manipulate an application's behavior to connect to the

Internet without firewall alerts.

- **Direct Network Access**

  This option protects you against the Trojan horses and other malicious programs that bypass network traffic.

  These programs penetrate the Windows TCP/IP layer to send and receive data without triggering firewall alerts.

- **Active Desktop Change**

  This option protects you against the malicious programs that use the documented interfaces that the trusted applications provide to transmit data outside the network without triggering firewall alerts.

- **Key Logger Monitor**

  This option protects you against the malicious keylogger programs that access personal information of a user on a particular computer by monitoring their keystroke activities.

	■ **COM Control** This option protects you against the malicious programs that manipulate an application's behavior by instantiating controlled COM objects.

About Norton Firewall Diagnosis

There may be times when firewall may block the network traffic that you want to allow based on its configuration settings. In such cases, you may have issues in accessing the Internet, the Network, or another computer to perform tasks such as sharing resources.

When you experience network connection problems, Norton Firewall acts quickly in identifying the cause of failure and provides its diagnosis. Norton Internet Security displays the **Firewall Diagnostics Wizard** when you encounter network connection problems.

Norton Firewall Diagnosis is available only in Windows 7.

The Wizard contains the problem diagnosis report that is unique for different cases of network blocks. For instance, a network block can occur in any of the following cases:

- The one click option to stop all network traffic is active
- The uncommon protocol that is handling the traffic is blocked
- The currently active firewall rule is conditioned to block the traffic that you want to allow
- The traffic has violated the process policy of the firewall

- The traffic has violated the traffic policy of the firewall
- The traffic comes from the restricted zone of networks or computers
- The traffic matches an Intrusion Prevention attack signature

You can use the **Firewall Diagnostics Wizard** as a guide to troubleshoot the network connection problem by yourself.

For each case of network block, the Wizard contains the firewall's analysis of the cause and the possible solutions to fix the block.

Norton Internet Security recommends that you use the **Firewall Diagnostics Wizard** to remove any type of block. The solutions in the Wizard let you analyze the issue and take a suitable action to resolve the problem.

Using the Wizard to troubleshoot the problem has the following advantages:

- It automatically tries to fix the problem by itself
- It lets you modify the settings that are related to the block
- It lets you view the log details related to the network block event
- It provides you the option to turn off firewall as the last means to resolve the issue

About Download Insight

Download Insight provides information about the reputation of any executable file that you download from the supported portals. The reputation details indicate whether the downloaded file is safe to install. You can use these details to decide the action that you want to take on the file.

Some of the supported portals are:

- Internet Explorer (Browser)

- Opera (Browser)
- Firefox (Browser)
- Chrome (Browser)
- AOL (Browser)
- Safari (Browser)
- Yahoo (Browser)
- MSN Explorer (Browser, E-mail & Chat)
- QQ (Chat)
- ICQ (Chat)
- Skype (Chat)
- MSN Messenger (Chat)
- Yahoo Messenger (Chat)
- Limewire (P2P)
- BitTorrent (P2P)
- Thunder (P2P)
- Vuze (P2P)
- Bitcomet (P2P)
- uTorrent (P2P)
- Outlook (E-mail)
- Thunderbird (E-mail)
- Windows Mail (E-mail)
- Outlook Express (E-mail)
- FileZilla (File Manager)
- UseNext (Download Manager)
- FDM (Download Manager)
- Adobe Acrobat Reader (PDF viewer)

Based on the type of portal you use to download your file, Norton Internet Security does one of the following:

- Analyzes the file based on its reputation details when the download is complete.
- Analyzes the file based on its reputation details when you try to run the file.

Download Insight uses the file analysis results to provide you the reputation details of the file. The basic reputation levels of the files are good, bad, unproven, and poor. Based on the reputation levels, the files can be broadly classified as follows:

Safe	Includes the files that are either Norton trusted or User trusted. Safe files have good reputation levels. These files do not harm your computer. By default, Auto-Protect allows the execution of the safe files.
Unsafe	Includes the files that Norton Internet Security identifies as a security risk or a threat. Unsafe files are characterized by bad or poor reputation levels and Norton Internet Security removes them from your computer.

Unknown	Includes the files that are neither safe nor unsafe. Unknown files have unproven reputation. These files might harm your computer. In the case of an unknown file, Download Insight notifies you that it is unsure of the reputation level of the file. You can use the **View Details** link in the notifications to view more details of the file. For unknown files, Norton Internet Security lets you decide the action that you want to perform on the file. For example, you can run a file, stop the file from running, install the file, cancel file installation, or remove the file from your computer.

By default, Download Insight lets you install safe files. For files of unknown reputation levels, Download Insight prompts you to select an action that you want to perform on the file. In case of an unsafe file, Download Insight informs you that Norton Internet Security has detected the file as a threat and has removed the file.

Based on the reputation details that the Download Insight notifications provide for the files that need attention, you can take an action on the file. The **Download Insight** window provides the various options that let you select an action. The options that appear in the window vary depending on the reputation level of the downloaded file. The following are some of the options that are available in this window:

Run this program	Lets you install the executable program.

Cancel installation	Lets you cancel the installation of the executable program.
Remove this file from my system	Lets you remove the file from your computer.

Security History logs details of all events that Download Insight processes and notifies. It also contains information about the safety level of the file and the action that you take on the file, if any. You can view these details in the **Download Insight** category in Security History.

When you turn off Auto-Protect, Norton Internet Security automatically turns off Download Insight. In this case, your computer is not adequately protected from Internet threats and security risks. Therefore, ensure that you always keep Auto-Protect turned on to protect your computer from security risks.

When Silent Mode is turned on, Norton Internet Security suppresses the Download Insight notifications.

Turning off or turning on Download Intelligence

Download Insight protects your computer against any unsafe file that you may run or execute after you download it using a supported Web browser. By default, the **Download Intelligence** option is turned on. In this case, Download Insight notifies you about the reputation levels of any executable file that you download. The reputation details that Download Insight provides indicate whether the downloaded file is safe to install.

There may be times when you want to turn off Download Insight. For example, if you want to download an unsafe file. In this case, you must turn off Download Insight so that Norton Internet Security lets you download the file and does not remove it from your computer.

You can use the **Download Intelligence** option to turn off or turn on Download Insight.

To turn off Download Intelligence

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Download Intelligence**.
4. In the **Download Intelligence** row, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Download Insight, and then click **OK**.
7. In the **Settings** window, click **OK**.

To turn on Download Intelligence

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Download Intelligence**.
4. In the **Download Intelligence** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

Configuring the Download Insight Notifications option

You can use the **Download Insight Notifications** option to choose when you want Download Insight to display notifications.

By default, the **Download Insight Notifications** option is set to **On**. Based on the type of portal you use to download your file, Norton Internet Security does one of the following:

- Notifies you each time when you download an executable file.

- Notifies you only when you download a file that is infected with a local virus identification. If the file that you download is infected with a cloud virus identification, Norton Internet Security removes the file from your computer and notifies you with the threat details.

When the **Download Insight Notifications** option is set to **Risks Only**, Download Insight notifies only when you download an infected or a suspicious executable file.

Setting the **Download Insight Notifications** to **Risks Only** does not turn off analysis of all the other executable files that you download. Whether or not you receive notifications of all files, Security History keeps a record of all the Download Insight activities. You can review the summary of the Download Insight alerts and notifications in Security History.

To configure the Download Insight Notifications option

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Download Intelligence**.
4. Under **Download Intelligence**, in the **Download Insight Notifications** row, do one of the following:
   - To receive Download Insight notifications only for the infected or the suspicious executable files that you download, move the **Download Insight Notifications** switch to the right to the **Risks Only** position.
   - To receive Download Insight notifications for all files that you download, move the **Download Insight Notifications** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

Configuring the Show Report on Launch of Files option

The **Show Report on Launch of Files** option lets you specify when and for what type of file you want to be prompted to select a suitable action. For example, you can specify the type of downloaded files for which Download Insight asks you to decide what to do with the file and how frequently these prompts for a suitable action must appear.

You can use the following options to configure **Show Report on Launch of Files**:

Always	When you set the **Show Report on Launch of Files** option to **Always**, Download Insight prompts you for a suitable action in case of safe and unknown files. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has a safe or an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. In the case of unsafe files, Norton Internet Security identifies them as threats and removes them.

Unproven Files Only	When you set the **Show Report on Launch of Files** option to **Unproven Files Only**, Download Insight prompts you to select a suitable action for unknown files only. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. By default, the **Show Report on Launch of Files** option is set to **Unproven Files Only**. In this case, Norton Internet Security allows the execution of the safe files without prompting you for a suitable action. In the case of unsafe files, Norton Internet Security identifies them as threat and removes them.

Never	When you set the **Show Report on Launch of Files** option to **Never**, Download Insight does not prompt you to select a suitable action for any type of file that you download. In this case, the **Download Insight** window does not appear whenever you try to launch any downloaded file. However, if the **Alert on Poor Stability** option is turned on, Download Insight prompts you to select a suitable action when you try to download an unstable file. In case of unsafe files, Norton Internet Security identifies them as threat and removes them. The alert messages that you suppress and the activity details can be reviewed at any time in Security History.

To configure the Show Report on Launch of Files option

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Download Intelligence**.

4 Under **Download Intelligence**, in the **Show Report on Launch of Files** row, do one of the following:
   - If you want Download Insight to prompt you for a suitable action in case of safe and unknown files, move the **Show Report on Launch of Files** switch to the **Always** position.
   - If you want Download Insight to prompts you to select a suitable action for unknown files only, move the **Show Report on Launch of Files** switch to the **Unproven Files Only** position.
   - If you do not want Download Insight to prompt you to select a suitable action for any type of file, move the **Show Report on Launch of Files** switch to the **Never** position.
5 In the **Settings** window, click **Apply**.
6 Click **OK**.

Turning on or turning off Alert on Poor Stability

When you turn on the **Alert on Poor Stability** option, Download Insight prompts you to select a suitable action when you try to download an unstable file.

When you set the **Show Report on Launch of Files** option to **Never**, Download Insight does one of the following:

- Does not prompt you to select a suitable action for any type of file that you download if the **Alert on Poor Stability** option is turned off. The **Download Insight** window does not appear whenever you try to open any downloaded file.
- Prompts you to select a suitable action when you try to download an unstable file if the **Alert on Poor Stability** option is turned on. Norton Internet Security identifies unsafe files as security threat and removes them.

By default, the **Alert on Poor Stability** option is turned off.

To turn on or turn off Alert on Poor Stability

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Download Intelligence**.
4. Under **Download Intelligence**, in the **Alert on Poor Stability** row, do one of the following:
   - To turn on **Alert on Poor Stability**, move the **On/Off** switch to the left to the **On** position.
   - To turn off **Alert on Poor Stability**, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

About Intrusion Prevention

Intrusion Prevention scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects your computer against most common Internet attacks.

For more information about the attacks that Intrusion Prevention blocks, go to the following URL:

http://www.symantec.com/business/security_response/attacksignatures

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way.

Intrusion Prevention scanning of every request from all the devices that access your computer increases the scan time which slows down the network speed of your computer. You can reduce the scan time and improve the network speed of your computer by excluding the trusted devices from Intrusion Prevention scanning.

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. These trusted devices can be excluded from Intrusion Prevention scan.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. Norton Internet Security runs LiveUpdate automatically to keep your list of attack signatures up to date. If you do not use Automatic LiveUpdate, you should run LiveUpdate once a week.

Turning off or turning on Intrusion Prevention notifications

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks. Whether or not you receive notifications, Intrusion Prevention activities are recorded in Security History. The Security History entries include information about the attacking computer and information about the attack.

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks based on a particular signature.

To turn off or turn on Intrusion Prevention notifications

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Intrusion Prevention**.
4. Under **Intrusion Prevention**, in the **Notifications** row, do one of the following:
   - To turn off notifications, move the **On/Off** switch to the right to the **Off** position.
   - To turn on notifications, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

To turn off or turn on an individual Intrusion Prevention notification

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Intrusion Prevention**.
4. Under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
5. In the **Intrusion Signatures** window, click an attack signature, and then click **Properties**.
6. In the **Signature Properties** window, uncheck or check **Notify me when this signature is detected**.
7. Click **OK**.
8. In the **Intrusion Signatures** window, click **OK**.

Excluding or including attack signatures in monitoring

In some cases, benign network activity may appear similar to an attack signature. You may receive repeated notifications about possible attacks. If you know that the attacks that trigger these notifications are safe, you can create exclusion for the attack signature that matches the benign activity.

Each exclusion that you create leaves your computer vulnerable to attacks.

If you have excluded the attack signatures that you want to monitor again, you can include them in the list of active signatures.

To exclude attack signatures from being monitored

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Intrusion Prevention**.
4. Under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
5. In the **Intrusion Signatures** window, uncheck the attack signatures that you want to exclude.

6 Click **OK**.

To include the attack signatures that were previously excluded

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Intrusion Prevention.**
4 Under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
5 In the **Intrusion Signatures** window, check the attack signatures that you want to include.
6 Click **OK**.

Turning off or turning on AutoBlock

When an attack attempt is detected, the connection is automatically blocked to ensure that your computer is safe. If the attack comes from a computer that has previously tried to access your computer by using another attack signature, Norton Internet Security activates AutoBlock. The AutoBlock feature blocks all traffic between your computer and the attacking computer for a specific time period. During this period, AutoBlock also blocks the traffic that does not match an attack signature.

AutoBlock stops traffic between your computer and a specific computer. If you want to stop all traffic to and from your computer, you can use the **Block All Network Traffic** option.

If AutoBlock blocks a computer or computers that you need to access, you can turn off AutoBlock.

To turn off or turn on AutoBlock

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Intrusion Prevention**.

4 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
5 In the **Intrusion AutoBlock** window, under **AutoBlock**, do one of the following:
   - To turn off Intrusion AutoBlock, click **Off**.
   - To turn on Intrusion AutoBlock, click **On (Recommended)**, and then in the **AutoBlock attacking computers for** drop-down list, select how long you want to turn on AutoBlock.
6 Click **OK**.

Unblocking AutoBlocked computers

In some cases, AutoBlock may recognize normal activity as an attack. The list of computers that AutoBlock has currently blocked may include the computer that you should be able to communicate with.

If a computer that you need to access appears on the list of blocked computers, you can unblock it. You may want to reset your AutoBlock list if you have changed your protection settings. To reset the AutoBlock list, you can unblock all of the computers that are on the list at one time.

To unblock AutoBlocked computers

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Intrusion Prevention**.
4 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
5 In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, do one of the following:
   - To unblock one computer, select its IP address, and then click **Unblock**.
   - To unblock all computers on the AutoBlock list, click **Unblock All**.

6 Click **OK**.

Permanently blocking a computer that has been blocked by AutoBlock

You can permanently block a computer that AutoBlock has blocked. The permanently blocked computer is removed from the AutoBlock list and added as a Restricted computer in the Network Security Map.

To permanently block a computer that has been blocked by AutoBlock

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Intrusion Prevention**.
4 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
5 In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, click the computer that you want to block permanently.
6 Click **Restrict**.
7 Click **OK**.

About Intrusion Prevention exclusion list

The Intrusion Prevention System in Norton Internet Security scans all the network traffic that enters and exits your computer. When a device on your network requests access to your computer, Intrusion Prevention scans this request to ensure that it is not a virus attack. If the information matches an attack signature, Intrusion Prevention blocks the traffic from the suspicious device and protects your computer. Scanning every request from all the devices that access your computer increases the scan time which slows down the network speed of your computer.

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. You can configure the trust level of a device

using the Network Security Map. You can exclude these trusted devices from Intrusion Prevention scan. Excluding Full Trust devices from the Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a device that is set to Full Trust, Norton Internet Security does not scan any information that is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

When a device on your network attempts to infect your computer, AutoBlock stops all access requests from this device. If you add this device to the Intrusion Prevention exclusion list, Norton Internet Security removes the device from the exclusion list.

Ensure that the IP address of the devices that are added to Intrusion Prevention exclusion list never changes.

If you find that any of the devices that you excluded from the Intrusion Prevention scan is infected, you can purge the saved exclusion list. When you purge the exclusion list, Norton Internet Security removes all the trusted devices from the exclusion list.

Removing all devices from Intrusion Prevention exclusion list

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. These trusted devices can be excluded from Intrusion Prevention scan. Excluding Full Trust devices from Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a Full Trust device from Intrusion Prevention scan, Norton Internet Security does not scan any information that is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

If you find that any of the devices that you excluded from Intrusion Prevention scan is infected, you can purge the saved exclusion list and remove all the devices.

You can purge the saved exclusion list under the following circumstances:

- Any of the devices that you excluded from Intrusion Prevention scan is infected.
- Any of the devices that you excluded from Intrusion Prevention scan attempts to infect your computer.
- Your home network is infected.

When a device on your network attempts to infect your computer, AutoBlock stops all the access requests from this device. If you add this device to the Intrusion Prevention exclusion list, Norton Internet Security removes the device from the exclusion list.

When you remove all the devices from the saved exclusion list, Intrusion Prevention scans every request from all the devices that access your computer.

To remove all the devices from the Intrusion Prevention exclusion list

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Intrusion Prevention**.
4. Under **Intrusion Prevention**, in the **Exclusion List** row, click **Purge**.
5. In the confirmation dialog box, click **Yes**.
6. In the **Settings** window, click **OK**

About Vulnerability Protection

Vulnerability Protection is a component of Intrusion Prevention System. Vulnerability Protection provides information about the susceptibility of the programs that may be on your computer against malicious

attacks. It also provides information about the known attacks that they are protected from.

Vulnerabilities are flaws in your programs or your operating system that can create weaknesses in overall security of your system. Improper computer configurations or security configurations also create vulnerabilities. External attackers exploit these vulnerabilities and perform malicious actions on your computer. Examples of such malicious attacks are active desktop monitoring, keylogging, and hacking. Such attacks can slow down the performance of your computer, cause program failure, or expose your personal data and confidential information to the hackers.

Norton Internet Security provides the signature-based solutions to protect your computer from the most common Internet attacks. Attack signatures contain the information that identifies an attacker's attempt to exploit a known vulnerability in your operating system or your computer programs. The Intrusion Prevention feature of Norton Internet Security uses an extensive list of attack signatures to detect and block suspicious network activity.

Vulnerability Protection lets you view the correlation between the vulnerabilities that your computer is protected against and the programs that may contain these vulnerabilities. For example, if Internet Explorer does not handle certain HTTP responses, it can result in a vulnerability that can be exploited. In this case, Vulnerability Protection lists Internet Explorer as a vulnerable program. It also provides details about the signatures that Intrusion Prevention uses to detect any attempt to exploit this vulnerability.

Viewing the list of vulnerable programs

The **Vulnerability Protection** window lets you view the extensive list of programs with the known vulnerabilities that Norton Internet Security protects you against.

For each program, you can view details such as the name of the program, its vendor, and the number of vulnerabilities that the program contains. You can also view more details about the vulnerabilities by clicking on the program name.

To view the list of vulnerable programs

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Network Protection** pane, click **Vulnerability Protection**.
3. In the **Vulnerability Protection** window, view the list of vulnerable applications.
4. After you finish viewing the list, click **Close**.

Viewing details about a vulnerable application

The **Vulnerability Protection** window displays the list of the programs on your computer that are susceptible to malicious attacks. In addition, you can view details of the vulnerabilities that a program contains. The **Program Vulnerability Details** window displays the names of the attack signatures that Intrusion Prevention uses to detect any attempts to exploit the vulnerabilities in the program.

You can click an attack signature to get additional information about the signature in the Symantec Security Response Web site.

The **Intrusion Signatures** window of **Intrusion Prevention** lets you view a list of attack signatures. Intrusion Prevention relies on this list of attack signatures to detect and block suspicious activity. You can uncheck a signature from the list, if you do not want Norton Internet Security to monitor the signature. The **Program Vulnerability Details** list does not include any signature that you disable in the **Intrusion Signatures** window. By default, all the signatures in the **Intrusion Signatures** window are turned on. Unless you have a good reason to disable a signature, you

should leave the signatures turned on. If you disable a signature, your computer may be vulnerable to attack.

To view details about a vulnerable application

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Network Protection** pane, click **Vulnerability Protection**.
3. In the **Vulnerability Protection** window, in the **Program** column, click the program name for which you want to view the details.
4. In the **Program Vulnerability Details** window, view the signature details of the program.
5. If you want to view additional information about the signature, then click the signature name.
6. After you finish viewing the vulnerability details, in the **Program Vulnerability Details** window, click **Close**.
7. In the **Vulnerability Protection** window, click **Close**.

About the types of security risks

Security risks, such as spyware and adware, can compromise your personal information and privacy. Spyware and adware programs are closely related. In some cases, their functionalities might overlap; but while they both collect information about you, the types of information that they collect can differ.

Spyware programs might put you at risk for identity theft or fraud. These programs might log your keystrokes, capture your email and instant messaging traffic. These programs also steal sensitive personal information such as passwords, login IDs, or credit card numbers. These programs can then send your compromised data to other people.

Adware displays advertisements on your computer and collects information about your Web browsing habits.

It then gives this data to companies that can send you advertisements based on these preferences.

Tracking cookies are the small files that programs can place on your computer to track your computing activities. Tracking cookies can then report that information back to a third party.

Some programs rely on other programs that are classified as security risks to function. For example, a shareware or freeware program that you download might use adware to keep its price low. In this case, you might want to allow the security risk program to remain on your computer. Also, you might need to restore the security risk program if Spyware Protection has removed it.

Norton Internet Security allows joke programs and other low-risk items to be installed on your computer by default. You can change your settings in the **Settings** window so that Norton Internet Security detects these security risks.

Checking Antispyware settings

While the default settings provide maximum protection from spyware, adware and other security risks, these settings are customizable.

To check Antispyware settings

1. In the Norton Internet Security main window, click **Settings**.
2. Under **Real Time Protection**, in the **Antispyware** row, click **Configure**.
3. In the **Antispyware** window, check the category of security risks that you want Antispyware to detect.
4. Click **OK**.

About Norton AntiSpam

Norton AntiSpam lets you categorize the email messages that you receive in your email programs into

spam email and legitimate email. It filters legitimate email into the Inbox folder and spam email into the Junk folder or the Norton AntiSpam folder.

Norton AntiSpam uses Symantec enterprise-class, spam-filtering technology to classify the spam email messages from legitimate email messages. Norton AntiSpam uses a real-time filter delivery mechanism and filters email messages using various local filters at different levels. The local filters classify the email messages as spam or legitimate. If the local filters classify the email message as legitimate, Norton AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Symantec Web server for additional analysis.

When the email message is classified as spam, Norton AntiSpam changes the subject of the email message and sends it to your email client. The email client identifies the change in the subject of the email message and moves it to the Junk folder or the Norton AntiSpam folder.

The Norton AntiSpam local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as spam or legitimate. For these filters to work efficiently, Norton AntiSpam requires antispam definition updates at regular intervals through LiveUpdate. These updates contain signature information of spam and legitimate email messages. The updates also contain any new rule that Symantec creates to filter spam email messages.

Norton AntiSpam uses predefined email rules and the user-defined Allowed List and Blocked List, to expedite the scanning of email. It accepts email messages from the list of allowed email senders and blocks email messages from the list of blocked email senders.

Norton AntiSpam also automatically imports the lists of addresses from supported email programs during the initial integration. It helps you keep your list of allowed and blocked email senders in sync with your

current address books. When Norton AntiSpam imports the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Turning off Norton AntiSpam increases your exposure to receive unsolicited email messages. Always ensure that Norton AntiSpam is turned on. It secures your email client from unwanted online content.

You can review all the antispam statistics under the **AntiSpam** category in the **Security History** window.

About Norton AntiSpam settings

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

Norton AntiSpam incorporates several powerful features to reduce your exposure to unwanted online content.

Norton AntiSpam settings help you configure the following:

- The email client with which Norton AntiSpam should integrate
- The list of allowed email senders
- The list of blocked email senders
- The email addresses and domains that Norton AntiSpam should not import into the list of allowed and blocked email senders
- The option to send feedback to Symantec about misclassified email
- The option to filter email messages through Web Query to maintain high spam detection efficiency

Configuring Client Integration

The Client Integration window lists the supported email programs, or clients, that are installed on your computer and their associated address books. When you select an email program, Norton Internet Security adds a **Norton AntiSpam** drop-down list or a few options to the toolbar of the supported email program. You can use the **Norton AntiSpam** drop-down list or the options to classify the email messages as spam or legitimate. You can also use these options to empty the spam folder and to open the **Settings** window to configure the Norton AntiSpam settings. If your email program does not have a Junk folder, it also adds a Norton AntiSpam folder in the folders area. You can use the Norton AntiSpam folder to sort and store spam messages. However, if your email client has a Norton AntiSpam folder from the previous version of Norton Internet Security, Norton AntiSpam uses the Norton AntiSpam folder and not the Junk folder.

Integration of Norton AntiSpam toolbar is not supported in Windows Mail in Windows Vista.

When you classify an email message as spam or legitimate, Norton AntiSpam lets you send the misclassified email message as feedback to Symantec. You can use the **Feedback** option to send the misclassified email message to Symantec for analysis.

You can also import the list of addresses that are present in the supported email program into the Norton AntiSpam Allowed List and Blocked List. Norton AntiSpam automatically adds the new email addresses from the address book of your supported email program once in a day when your computer is idle. However, if you want to manually import addresses, use the **Import** option in the **Allowed List** window.

When you open your email client, the welcome screen appears. If you do not want the welcome screen to appear in the future, check the **Don't show this again** option before you click **Close**. Norton Internet Security

notifies the successful integration of Norton AntiSpam with your email client.

Norton AntiSpam also automatically imports the lists of addresses from the supported email programs during the initial client integration. It helps you keep your list of allowed and blocked email senders in sync with your current address books. When Norton AntiSpam imports the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Norton Internet Security supports Norton AntiSpam integration with the following email programs:

- Microsoft Outlook 2002/2003/2007/2010
- Outlook Express 6.0 or later
- Windows Mail in Windows Vista

Norton Internet Security supports only the 32-bit version of Microsoft Outlook 2010.

Norton Internet Security does not add any options to the Windows Mail toolbar. However, it identifies the spam email messages and moves them into the Junk folder or the Norton AntiSpam folder.

After successful integration, Outlook Express restarts automatically.

To configure Client Integration

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. Under **AntiSpam**, in the **Client Integration** row, click **Configure**.
5. In the **Client Integration** window, check the programs with which you want Norton AntiSpam to integrate.
6. Select one or more address books to be imported automatically into your Allowed List.

7 Click **OK** to save the changes and close the **Client Integration** window.

Setting Address Book Exclusions

When you add an email address to the Address Book Exclusions list, Norton AntiSpam does not import the address into the Allowed List and Blocked List. If you delete an email address from the Allowed List or Blocked List, Norton AntiSpam automatically adds the address to the Address Book Exclusions list. However, when you delete an email address that you manually added to the Allowed List or Blocked List, Norton AntiSpam does not add the address to the Address Book Exclusions list.

You cannot add a domain name to the Address Book Exclusions list. When you delete a domain name from the Allowed List or Blocked List, Norton AntiSpam does not add the domain name to the Address Book Exclusions list.

You can specify Address Book Exclusions before you import the address book. Add all email addresses to the Address Book Exclusions list that you do not want to import from the address book of your email program.

To add entries to the Address Book Exclusions list

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Message Protection**.
4 Under **AntiSpam**, in the **Address Book Exclusions** row, click **Configure**.
5 In the **Address Book Exclusions** window, click **Add**.
6 In the **Add Email Address** dialog box, type the email address.
Optionally, type the name that corresponds to the email address for easy identification.
7 Click **OK** to close the **Add Email Address** dialog box.

8 Click **OK** to save and close the **Address Book Exclusions** window.

To edit or delete entries in the Address Book Exclusions list

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Message Protection**.
4 Under **AntiSpam**, in the **Address Book Exclusions** row, click **Configure**.
5 In the **Address Book Exclusions** window, select the item with which you want to work.
6 Do one of the following:
   - To edit an entry, click **Edit** to open the **Edit Email Address** window, edit the details, and then click **OK**.
   - To delete an entry, click **Remove**.
7 Click **OK** to save and close the **Address Book Exclusions** window.

Identifying authorized senders

When you know that you want to receive any email messages from a specific address or domain, you can add it to the Allowed List.

Norton AntiSpam automatically imports the address book entries and Safe Sender List entries once in a day when your computer is idle.

If you have added a new supported email program, you can import its address book manually to your Allowed List immediately or at any time. You can also add names and domains to the Allowed List individually.

Before you import the address book, you can specify your Address Book Exclusions. Norton AntiSpam does not import the email addresses that you add to the Address Book Exclusions list.

To import an address book

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. Under **AntiSpam**, in the **Allowed List** row, click **Configure**.
5. In the **Allowed List** window, click **Import**.
6. Click **OK** to save and close the **Allowed List** window.

To add entries to your Allowed List

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection.**
4. Under **AntiSpam**, in the **Allowed List** row, click **Configure**.
5. In the **Allowed List** window, click **Add**.
6. In the **Add Email Address** dialog box, in the **Address Type** drop-down list, specify whether you add an email address or a domain name.
7. Do one of the following:
   - To add an email address, type the email address that you want to allow, and optionally, the name of the sender.
   - To add a domain name, type the address of the domain (for example, symantec.com), and optionally, the name of the domain.
8. Click **OK** to close the **Add Email Address** dialog box.
9. Click **OK** to save and close the **Allowed List** window.

To edit or delete entries in the Allowed List

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.

4 Under **AntiSpam**, in the **Allowed List** row, click **Configure**.
5 In the **Allowed List** window, select the item with which you want to work.
6 Do one of the following:
   - To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and click **OK**.
   - To delete an entry, click **Remove**.

     When you delete an entry that was imported, Norton AntiSpam automatically adds it to the Address Book Exclusions list.
7 Click **OK** to save and close the **Allowed List** window.

Identifying senders of spam

If you do not want to receive any email messages from a specific address or domain, you can add it to the Blocked List. Norton AntiSpam marks all email messages from this address or domain as spam.

Norton AntiSpam also automatically imports the lists of addresses that are available in the Blocked Sender lists of your email program into the Blocked List during the initial client integration or address book import.

Norton AntiSpam lets you type invalid email addresses to the Blocked List.

Always add unknown email addresses and domains to the Blocked List, so that you do not receive unsolicited email messages from such addresses or domains.

To import addresses to the Blocked List

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Message Protection**.
4 Under **AntiSpam**, in the **Allowed List** row, click **Configure**.
5 In the **Allowed List** window, click **Import**.

6 Click **OK** to save and close the **Allowed List** window.

To add entries to the Blocked List

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Message Protection**.
4 Under **AntiSpam**, in the **Blocked List** window, click **Configure**.
5 In the **Blocked List** window, click **Add**.
6 In the **Add Email Address** dialog box, in the **Address Type** drop-down list, specify whether you add an email address or a domain name.
7 Do one of the following:
   - To add an email address, type the email address that you want to block, and the name of the sender.
   - To add a domain, enter the address of the domain (for example, symantec.com), and the name of the domain.
8 Click **OK** to close the **Add Email Address** dialog box.
9 Click **OK** to save and close the **Blocked List** window.

To edit or delete entries in the Blocked List

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Message Protection**.
4 Under **AntiSpam**, in the **Blocked List** window, click **Configure**.
5 In the **Blocked List** window, select the item with which you want to work.

6 Do one of the following:

- To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and then click **OK**.
- To delete an entry, click **Remove**.

  When you delete an entry that was imported, Norton AntiSpam automatically adds it to the Address Book Exclusions list.

7 Click **OK** to save and close the **Blocked List** window.

About your email program toolbar

Norton AntiSpam adds a drop-down list or a few options to the toolbar of supported email programs.

Integration of Norton AntiSpam toolbar is not supported in Windows Mail in Windows Vista.

You can use the following options:

This is Spam	Marks the selected email as spam and moves the email message into the Junk folder or the Norton AntiSpam folder. When you reclassify an email message as spam, Norton Internet Security provides you the option to send the misclassified email message as feedback to Symantec. This option appears only if the **Feedback** option in the **Message Protection** section of the **Settings** window is set as **Ask Me**. The **Message Protection** section is available in the **Network** tab. When you reclassify an email message as spam, Norton Internet Security displays a message whether or not to add the sender's email address to the Blocked List. This message appears depending on the option that you select in the drop-down list present at the bottom of the **Blocked List** window.

This is not Spam	Marks the selected email as allowed (not spam) and moves the email message into the **Inbox**. When you reclassify an email message as legitimate, Norton Internet Security provides you the option to send the misclassified email message as feedback to Symantec. This option appears only if the **Feedback** option in the **Message Protection** section of the **Settings** window is set as **Ask Me**. The **Message Protection** section is available in the **Network** tab. When you reclassify an email message as legitimate, Norton Internet Security displays a message whether or not to add the sender's email address to the Allowed List. This message appears depending on the option that you select in the drop-down list present at the bottom of the **Allowed List** window.
Empty Spam Folder	Removes all email that has been placed in the Junk folder or the Norton AntiSpam folder.
Open Norton AntiSpam	Displays the **Message Protection** section of the **Settings** window. The **Message Protection** section is available in the **Network** tab.

Setting the Feedback option

Email messages in the email client might sometimes get wrongly classified as spam or legitimate. The **Feedback** option lets you send the misclassified email message as feedback to Symantec for analysis.

The **Feedback** option is available only when Microsoft Outlook or Outlook Express is installed on your computer.

To set the Feedback option

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. Under **AntiSpam**, in the **Feedback** row, select any one from the following three options:

On	Automatically sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Ask Me	Prompts you before Norton AntiSpam sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Off	Does not send the misclassified email message to Symantec

5. Click **OK** to save and close the **Settings** window.

About Web Query

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images. The Web Query is a feature of Norton AntiSpam that Norton Internet Security uses to classify the email messages more effectively.

An effective spam filtration is possible when each email message that you receive is scanned through different filters. With only one or two levels of email filters, a

high percentage of legitimate emails are misclassified as spam or spam is misclassified as legitimate. To avoid such misclassification, Norton AntiSpam employs different filters. Each email filter uses a unique approach to filter spam email messages from legitimate email messages.

The email messages that you receive in your email program undergo scanning through different local filters of Norton AntiSpam. The local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as legitimate or spam. If the local filters classify an email message as spam, Norton AntiSpam changes the subject of the email message. Norton AntiSpam then sends the email message to your email client. If the local filters fail to classify the email message as spam, Norton AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Web Query filter for additional analysis.

The Web Query filter analyzes the signature and URL hashes of the email message and then sends the analysis report to Norton AntiSpam. If the email message is identified as spam, Norton AntiSpam alters the subject of the email message and sends it to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends that you keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

You can turn on or turn off the **Web Query** option in the Norton Internet Security **Settings** window.

Turning off or turning on Web Query

Norton AntiSpam uses local filters to identify spam email messages. The email messages that the local filters do not identify as spam are then scanned

additionally through the Web Query filter. Web Query filter analyzes the signature and URL hashes of the email messages to classify them as legitimate email or spam email.

If the email message is identified as spam, then Norton AntiSpam alters the subject of the email message. Norton AntiSpam then sends the email message to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends you to keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

To turn off the Web Query filter

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. Under **AntiSpam**, in the **Web Query** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **OK** to save and close the **Settings** window.

To turn on the Web Query filter

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. Under **AntiSpam**, in the **Web Query** row, move the **On/Off** switch to the left to the **On** position.
5. Click **OK** to save and close the **Settings** window.

About configuring POP3 and SMTP ports

Norton Internet Security automatically configures your email program to protect it from viruses and other security threats. Norton Internet Security supports all

email programs that use non-SSL POP3 and SMTP communication protocols. Norton Internet Security also scans all incoming and outgoing email messages.

Norton Internet Security lets you manually configure your POP3 and SMTP email ports for email protection. Typically, your Internet service provider (ISP) provides you the port numbers for your email program. If the SMTP and POP3 port numbers for your email program are different from the default port numbers, you must configure Norton Internet Security.

To ensure email protection, Symantec recommends that you check the POP3 and SMTP port numbers for your email program. If they are not the default ports, add them to the **Protected Ports** window. To configure the **Protected Ports Settings** option, go to the Norton Internet Security main window, and then click **Settings > Network > Message Protection > Protected Port Settings > Configure**.

If you do not want Norton Internet Security to protect a port, you can remove the port from the **Protected Ports** window.

You cannot remove the default SMTP port 25 and POP3 port 110. Norton Internet Security automatically protects these default ports.

Adding POP3 and SMTP ports to Protected Ports

Norton Internet Security supports all email programs that use POP3 and SMTP communication protocols with default ports. However, if your email program is not configured with the default ports, you can manually configure your POP3 and SMTP email ports.

To ensure email protection, the POP3 and SMTP port numbers must be protected. If the POP3 and SMTP port numbers are not the default ports, Symantec recommends that you add the port numbers to the **Protected Ports** window.

To add POP3 and SMTP ports to Protected Ports

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. In the **Protected Ports Settings** row, click **Configure**.
5. In the **Protected Ports** window, click **Add**.
6. In the **Add Port to protect** window, in the **Port Type** drop-down list, do one of the following:
   - To add the incoming email port, click **POP3**.
   - To add the outgoing email port, click **SMTP**.
7. In the **Port** box, type the port number.
   The port number must be between 1 and 65535.
8. Click **OK**.
9. In the **Protected Ports** window, click **Apply**, and then click **OK**.
10. In the **Settings** window, click **OK**.

Removing an email port from Protected Ports

If you do not want Norton Internet Security to protect a port, you can remove the port from the **Protected Ports** window.

Norton Internet Security automatically protects the default SMTP port 25 and the default POP3 port 110. You cannot remove these default ports.

To remove an email port from Protected Ports

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. In the **Protected Ports Settings** row, click **Configure**.
5. In the **Protected Ports** window, click the port that you want to remove, and then click **Remove**.

6 Click **Apply** and then click **OK**.
7 In the **Settings** window, click **OK**.

About the Network Security Map

A home network typically consists of the computers and other devices that share your Internet connection. The Network Security Map helps you view and manage your network.

After you configure Network Security Map, Norton Internet Security automatically detects the devices that are connected to your network and lists them in the Network Security Map. You can view devices and customize the Network Security Map to remotely monitor the computers on which a Norton product is installed.

Ensure that the computers that you want to remotely monitor have a version of a Norton product that supports Remote Monitoring.

You can monitor the following items in the Network Security Map:

- Security status of the computers that are connected to the network
- Status of the protection features of the computers that are connected to the network
- Subscription status and Norton product version of the computers that are connected to your network
- Status of your wireless network connection
- Connection status of the devices that are on the network
- The known, unknown, or intruder devices that are on your network

You can grant or deny permission to the networked devices to access your computer.

You can also modify details about a computer or device that is connected to your network.

Turning off or turning on Network Security Overview

The **Network Security Overview** window provides a brief summary about the following features:

- Wireless Security
- Remote Monitoring
- Network Map
- Trust Controls

You can click each of the features and read the summary to learn more about using Network Security Map to manage your home network. By default, the **Network Security Overview** window appears each time you open **Network Security Map**.

If you do not want to view the **Network Security Overview** window, you can turn it off. Turning off the **Network Security Overview** window does not affect the performance or security of your computer.

You can also turn off the **Network Security Overview** window if you check **Do not show this again** option that is available at the bottom of the **Network Security Overview** window.

To turn off Network Security Overview

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Network Security Settings**.
4. In the **Welcome Screen** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **Apply**.
6. Click **OK**.

To turn on Network Security Overview

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Network Security Settings**.

4 In the **Welcome Screen** row, move the **On/Off** switch to the left to the **On** position.
5 Click **Apply**.
6 Click **OK**.

Viewing devices on the Network Security Map

The **Network Security Map** window provides a pictorial representation of the devices on the network to which your computer is connected. You can view the details of each device, such as device name, security status, and IP address.

The **Network Security Map** window also provides the security status of the following computers:

- The computer on which you view the remote monitoring status (MY PC)
- The computers that are remotely monitored

The trust level of the device appears at the bottom of the icon in the network map.

Norton Internet Security displays devices in the following order:

- MY PC
- Devices with online connection status
- Devices with offline connection status

When you connect a new device to your network, Norton Internet Security automatically refreshes the **Network Security Map** window and displays the device.

Norton Internet Security requires you to configure the Symantec Security Driver to open the Network Security Map. You cannot install the Symantec Security Driver when you run LiveUpdate. You can either allow the Norton LiveUpdate to complete or close the Norton LiveUpdate session before you install the Symantec Security Driver.

To view devices on the Network Security Map

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. If the **Product Configuration** panel appears, click **Continue**.
   The **Product Configuration** panel appears when you click **Network Security Map** for the first time. The **Product Configuration** panel helps you install Symantec Security Driver that is required to view the **Network Security Map** window. The process of installation of the Symantec Security Driver disrupts your network connection temporarily.
4. If the **Network Security Overview** window appears, click **OK**.
   The **Network Security Overview** window lets you view the summary of features of the Network Security Map. The **Network Security Overview** window appears in the following instances:
   - When you open the **Network Security Map** window for the first time
   - When you turn on **Welcome Screen** under **Network Security Map** in the **Settings** window

   If you do not want to view the **Network Security Overview** window in the future, check **Do not show this again** before you click **OK**.
5. In the **Network Details** drop-down list, select the network that lists the device for which you want to see the details.

To view the details of a device on the Network Security Map

❖ In the **Network Security Map** window, click a device icon.
You can use the scroll arrows to view the devices that are listed in the network map.
The device details section that is located below the network map displays the following details:

Device Name	Shows the name of the device For a computer, the Network Security Map displays the NetBIOS name by default. However, the Network Security Map displays the name of the device as NEW if it meets the following conditions: ▪ The device does not have a NetBIOS name ▪ The device has a firewall that is enabled You can change the device name in the **Edit Device Details** window.
Adapter Manufacturer	Shows the name of the network adapter manufacturer of the device The adapter manufacturer's name is based on the physical address (also known as Media Control Access address or MAC address) of the device.

Category	Shows the category to which the device belongs The device category icon provides details on the connection status and security status. Norton Internet Security labels all unknown devices as NEW and sets the category as GENERIC DEVICE. This category may include computer-related devices, such as printers, media devices, and game consoles. You can change the device category in the **Edit Device Details** window.
Security Status	Shows how well your computer is protected from threats, risks, and damage The security status appears only for **MY PC** and the computers that are remotely monitored.
Remote Monitoring	Shows the connection status of Remote Monitoring The statuses are: ON OFF You can turn off Remote Monitoring for an individual computer or for all the computers that you remotely monitor.

Trust Level	Shows the access level that is granted to a remote device to connect to your computer The initial trust level is set based on the configuration of your computer. You can set trust level for all devices other than **MY PC**.
Connection	Shows the status of the connection The statuses are: ▪ **ONLINE** ▪ **OFFLINE**
Physical Address	Shows the physical address (also known as the Media Access Control address or MAC address) of the computer or device
IP Address	Shows the IP address of the computer or device If you change the IP address of a device, the updated IP address appears in the **Network Security Map** window when you refresh the list.

Excluded from IPS scanning	Shows if the device is excluded from Intrusion Prevention scan. You can exclude a Full Trust device from Intrusion Prevention scan. When you exclude a trusted device from Intrusion Prevention scan, Norton Internet Security trusts this device and does not scan any information that is received from this device. This improves the network speed of your computer and helps the trusted device to access your device quickly.

Setting up Remote Monitoring

You can set up Remote Monitoring by allowing computers on your network to communicate with your computer.

Ensure that the computers that you want to remotely monitor have a version of a Norton product that supports Remote Monitoring.

Norton Internet Security requires a Passkey to set up Remote Monitoring. You must type the same Passkey for all the computers that you want to remotely monitor.

After you set up Remote Monitoring, you can connect any computer to your network and enter the same Passkey. Norton Internet Security automatically identifies the computer and connects it to the Network Security Map.

To set up Remote Monitoring

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.

3 On the left side of the **Network Security Map** window, under **Remote Monitoring**, click **Setup**.

4 In the **Remote Monitoring Setup** window, type a Passkey.
The Passkey should be between 6 and 20 characters in length. The Passkey is case sensitive.

5 Under **Choose the default mode for Computer Discovery**, select one of the following options:

Computer Discovery always on	Lets your computer always discover other computers that are connected to the network
Computer Discovery on only when Network Security Map screen is displayed	Lets your computer discover other computers that are connected to the network when the **Network Security Map** window is open

6 Click **OK**.

7 Set up Remote Monitoring for all other computers that you want to monitor remotely.

Turning off Remote Monitoring

When you turn off Remote Monitoring, you stop remote monitoring of the computers that are connected to your network.

You can turn off Remote Monitoring for the following:

- All of the computers that you remotely monitor
- An individual computer that you remotely monitor

You can turn off Remote Monitoring only after you complete the Remote Monitoring Setup process.

To turn off Remote Monitoring for all computers

1 In the Norton Internet Security main window, Click **Advanced**.

2 Under **Network Protection**, click **Network Security Map**.
3 On the left side of the **Network Security Map** window, under **Remote Monitoring**, click **Disable**.
4 In the confirmation dialog box, click **Yes**.

To turn off Remote Monitoring for an individual computer

1 In the Norton Internet Security main window, click **Advanced**.
2 Under **Network Protection**, click **Network Security Map**.
3 In the **Network Security Map** window, in the network map, click the computer for which you want to disable Remote Monitoring.
4 In the device details area, next to **Remote Monitoring**, click **Disable**.
5 In the confirmation dialog box, click **Yes**.

Adding a device to the Network Security Map

You can manually add a computer or device to the Network Security Map.

You can add the following details when you add a device:

- The name or description
- The IP address or physical address

The Network Security Map finds any computers that are connected to your network. However, you can add the computers and the devices that are currently not connected.

Norton Internet Security adds to the Trust Control network all the devices that you manually add to Network Security Map. You can select the Trust Control network in the **Network Details** drop-down list to view the devices that you added. You can also edit the name of the device.

You cannot edit the Trust Control network details.

The default trust level of the devices that you add to the Network Security Map is Protected. However, you can change the trust level of the devices.

If you trust a device that is not on your network, you can expose your computer to potential security risks.

To add a device to the Network Security Map

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. On the left side of the **Network Security Map** window, under **Total in Network**, click the plus symbol.
4. In the **Add a Device** window, in the **Name** box, type the name of the device that you want to add to the Network Security Map.
   The maximum character length of the device name is 15 characters.
5. In the **IP or Physical Address** box, type the IP address or physical address of the device that you want to add to the Network Security Map.
   You can use the following formats in the **IP or Physical Address** box:

IPv4 address	172.16.0.0
IPv6 address	fe80::12ac:fe44:192a:14cc
Physical address	11-22-c3-5a-fe-a4
Resolvable host	ftp.myfiles.com

   The address that you provide is not verified until the device is physically found on the network.
6. Click **Add Device**.

Finding a computer's IP address

You can find a computer's IP address in various ways. On Windows 2000/XP, Windows Vista, and Windows 7 computers, you can use Ipconfig to find the IP address of a computer.

Ipconfig reports the IP address of its local computer only. You must run this program on the computer that you want to identify.

To find an IP address by using Ipconfig on Windows 2000/XP

1. On the computer you want to identify, on the Windows taskbar, click **Start > Run**.
2. In the **Run** dialog box, type `cmd`.
3. Click **OK**.
4. At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
5. Write down the IP address.

To find an IP address by using Ipconfig on Windows Vista

1. On the computer you want to identify, on the Windows taskbar, click **Start**.
2. In the **Start Search** text box, type `cmd`, and then press **Enter** on your keyboard.
3. At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
4. Write down the IP address.

To find an IP address by using Ipconfig on Windows 7

1. On the computer you want to identify, on the Windows taskbar, click **Start**.
2. In the **Search programs and files** text box, type `cmd`, and then press **Enter** on your keyboard.
3. At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
4. Write down the IP address.

Editing device details

You can change the name and category of a device that is available on the Network Security Map. You can select the categories such as Generic Device, Laptop, Media Device, or Game Console.

You cannot change the category of the device that you added manually. By default, Norton Internet Security displays the category of the manually added device as **USER DEFINED**.

The **Network Security Map** window displays different icons, depending on the category that you select. Icons help you identify the devices that are listed in the network map.

To edit the details of the device that is on your network

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. In the **Network Security Map** window, in the network map, click a device icon.
4. In the device details section, next to **Device Name**, click **Edit**.
5. In the **Edit Device Details** window, in the **Name** box, type a new name.
   The maximum character length of the device name is 15 characters.

6 In the **Category** drop-down list, click one of the following device categories:
- **GENERIC DEVICE**
- **DESKTOP PC**
- **LAPTOP**
- **SERVER PC**
- **NETWORK PRINTER**
- **ROUTER/SWITCH**
- **CABLE/DSL MODEM**
- **MEDIA DEVICE**
- **GAME CONSOLE**
- **PDA/MOBILE PHONE**
- **NETWORK STORAGE DEVICE**
- **WEB CAMERA**

7 Click **OK**.

To edit the name of the device that you added manually

1 In the Norton Internet Security main window, click **Advanced**.
2 Under **Network Protection**, click **Network Security Map**.
3 In the **Network Security Map** window, in the **Network Details** drop-down list, click **Trust Control**.
4 In the network map, select a device that you added.
5 In the device details area, next to **Device Name**, click **Edit**.
6 In the **Edit Device Details** dialog box, in the **Name** box, type a new name.
7 Click **OK**.

Editing network details

You can view the details and change the name of your network in the **Edit Network Details** window.

You cannot edit the Trust Control network details.

To edit network details

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. In the **Network Security Map** window, on the right side of **Network Details**, click **Edit**.
4. In the **Edit Network Details** dialog box, in the **Network Name** box, type a new name.
5. Click **OK**.

Changing the trust level of your network and devices

The trust level determines the default level of access that devices on your network have to your computer. Any device on your network that is not explicitly Trusted or Restricted uses the trust level of your network. The initial network trust level is set based on the configuration of your computer.

Ensure that you change the trust level of a device to Full Trust, if it is a known device, and is connected to your network.

The following conditions are necessary for the trust level of a device to be Shared:

- The computer should not have a public IP address.

  Your computer does not have a public IP address if it is not directly connected to the Internet.
- The computer should be connected to a LAN through a secure connection.
- The network category should be private in Windows Vista.

In addition, the trust level of a device is Shared in any of the following cases:

- When the computer on the network has one or more folders or printers that are shared
- When the computer is Media Center compatible (for example, if you have Windows XP Media Center Edition, Windows Vista Home Premium, Windows

Vista Ultimate, Windows 7 Home Premium, Windows 7 Professional, or Windows 7 Ultimate)

If you use a wireless network that is not secure, the default trust level of all the devices that are on the network is **Protected**.

The trust level of a device also depends on the trust level of its network. When you change the trust level of a network, Norton Internet Security assigns the same trust level to all the devices that are connected to that network. However, Norton Internet Security does not change the trust level of the devices that you individually trust or restrict.

You can modify these settings if you want to change the trust level for the following:

- Your network
- Devices that are connected to the Network Security Map

To change the trust level of your network

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. In the **Network Security Map** window, on the right side of **Network Details**, click **Edit**.
4. In the **Edit Network Details** window, next to **Trust Level**, click **Edit**.
   You can view the details of the network in the **Edit Network Details** window before you change the trust level.

5 To select a trust level for a network, in the **Edit Network Trust Level** window, click one of the following:

FULL TRUST	Adds the network to the Trusted list All the network traffic that your computer receives from a Trusted network is filtered and allowed through firewall. However, known attacks and infections are still monitored. You should select this setting only when you are sure that the network is completely safe.
SHARED	Adds the network to the Shared list All the network traffic that your computer receives from a Shared network is filtered. Only shared resources on your computer, such as files, folders, and printers are allowed. You should select this setting if you want the firewall to protect you from all traffic except those that pertain to file and printer sharing.
PROTECTED	Adds the network to the Protected list A network is in the Protected Trust Level when it has not been classified as Trusted, Shared, or Restricted. You remain protected from known attacks and all unexpected traffic.

RESTRICTED	Adds the network to the Restricted list The devices that are on Restricted network cannot communicate with your computer. However, you can still use the network to browse Web sites, send email messages, or transmit other communications.

6 Click **OK**.

To change the trust level of a device

1 In the Norton Internet Security main window, click **Advanced**.

2 Under **Network Protection**, click **Network Security Map**.

3 In the **Network Security Map** window, do one of the following:

- To edit the trust level of a device that is on your network, in the network map, click the device.
- To edit the trust level of a device that you manually added, in the **Network Details** drop-down list, click **Trust Control**, and then click the device.

4 In the device details section, next to **Trust Level**, click **Edit**.

5 To select a trust level for a device, in the **Edit Device Trust Level** window, click one of the following:

FULL TRUST	Adds a device to the Full Trust list Full Trust devices are monitored only for known attacks and infections. You should select this setting only when you are sure that the device is completely safe.
RESTRICTED	Adds a device to the Restricted list Restricted devices do not have access to your computer.
USE NETWORK TRUST (trust level)	Adds a device to a default trust level The devices that are removed from the Full Trust level or Restricted trust level take the default trust level of the network. The trust level of the network can be Full Trust, Restricted, Protected, or Shared.

6 Click **OK**.
Norton Internet Security displays the trust level status of each restricted device on the icon of the device.

Excluding a device from Intrusion Prevention scan

The Intrusion Prevention System in Norton Internet Security scans all the network traffic that enters and exits your computer. When a device on your network requests access your computer, Intrusion Prevention scans this request to ensure that it is not a virus attack.

Scanning every request from all the devices that access your computer increases the scan time which slows down the network speed of your computer.

If you know that a specific device on your network is safe, you can apply Full Trust level to this device. In addition, you can exclude this specific device from Intrusion Prevention scan. When you exclude a device from Intrusion Prevention scan, Norton Internet Security trusts this device and does not scan any information that is received from this device. This improves the network speed of your computer and helps the trusted device to access your device quickly.

You can exclude only full trusted devices that are on the local subnet.

To exclude a device from Intrusion Prevention scan, you must ensure that the IP address of the device never changes. Norton Internet Security uses IP addresses to identify devices on your home network. If the IP address of the device changes, Norton Internet Security cannot identify the trusted device that should be excluded from Intrusion Prevention scan.

You can exclude a trusted device from Intrusion Prevention scan only if you are sure that the device does not have any security threats.

When you apply Full Trust to a device and exclude it from Intrusion Prevention scan, the IP address and MAC address of the device are added to the Trust Control.

To exclude a device from Intrusion Prevention scan

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. If the **Network Security Overview** window appears, click **OK**.

4 In the **Network Security Map** window, do one of the following:
   - To edit the trust level of a device that is on your network, in the network map, click the device.
   - To edit the trust level of a device that you manually added, in the **Network Details** drop-down list, click **Trust Control**, and then click the device.
5 In the device details section, in the **Trust Level** row, click **Edit**.
6 In the **Edit Device Trust Level** window, click **FULL TRUST**.
7 At the bottom of the **Edit Device Trust Level** window, check **Exclude from IPS scanning**.
8 In the **Exclude from IPS Scanning** dialog box, click **Yes** to confirm.
9 Click **OK**.

Removing devices from the Network Security Map

The **Network Security Map** window lists the devices that are connected to your network. You can remove a device or a computer from the Network Security Map. You can purge all devices from the network map and create a new list of devices. For example, you can purge all the devices that were present in your previous network before you connect to a new network. Ensure that you disable Remote Monitoring before you purge the network map. Norton Internet Security cannot purge the network map when the Remote Monitoring is turned on. Also, ensure that you close the **Network Security Map** window before you purge the network map. You cannot purge the network map when the **Network Security Map** window is open.

Norton Internet Security purges the devices that you add manually in the Trust Control network depending upon their trust level. It does not purge the devices that have a trust level as Full Trust or Restricted.

When you remove an individual device, the online devices appear again the next time you open the Network Security Map. However, Norton Internet Security permanently removes the offline devices.

To remove an individual device

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. In the **Network Security Map** window, do one of the following:
   - To remove a device that is on your network, in the network map, click the device.
   - To remove a device that you manually added, in the **Network Details** drop-down list, select **Trust Control**, and then click the device.
4. On the left side of the **Network Security Map** window, under **Total in Network**, click the minus symbol.
5. In the confirmation dialog box, click **Yes**.

To purge the Network Security Map

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Network Security Settings**.
4. In the **Network Security Map** row, click **Purge**.
5. In the confirmation dialog box, click **Yes**.

Viewing the status of your wireless network

You can view the status of your wireless network in the **Network Security Map** window. The Network Security Map displays the status of your wireless network as secure or not secure. A secure network requires a strong wireless encryption. If your wireless network is not secure, you can turn on encryption on your wireless router.

For more information on how to secure your wireless network, on the left side of the **Network Security Map** window, click the **Why is it not secure** link. Follow the instructions.

You should only trust a wireless connection that is secure. Trusting a wireless connection that is not secure puts all of the devices on your network at risk.

To view the status of your wireless network

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. On the left side of the **Network Security Map** window, view the status of your wireless network. Your wireless network statuses are:

Wireless Network Secure	Indicates that your wireless network is secure
Wireless Network Not Secure	Indicates that your wireless network is not secure

Viewing the device details

The Network Security Map lets you view the details of the computers that you remotely monitor. You can view the following details:

- The configuration status of your protection features, such as Auto-Protect, Intrusion Prevention, and Email Scanning
- The configuration status of your definition updates, such as Automatic LiveUpdate and Pulse Updates
- The version number of your Norton product
- The subscription status of your Norton product
- The configuration status of your transaction security, such as Identity Safe and Antiphishing

To view the device details

1. In the Norton Internet Security main window, click **Advanced**.
2. Under **Network Protection**, click **Network Security Map**.
3. In the **Network Security Map** window, in the network map, click the device for which you want to see the details.
   You can view the details of only the computers that you remotely monitor.
4. In the device details section, next to **Category**, click **Details**.
5. In the **Device Details** window, view the details of the device.
6. Click **Close**.

Modifying the communication port for Network Security Map

The Network Security Map settings lets you configure the communication port number that Norton products use to communicate with each other over a network. By default, Norton products use 31077 as the communication port number.

If you change the communication port number of your Norton product, you must change it on every computer that is connected to your home network. In addition, when you find more computers that use the **Remote Monitoring Setup** process, ensure that the same port number is used on every computer.

Though you can modify the communication port number, it is recommended that you do not change this port number. If you change the communication port number, you must use a port number in the range of 1-65535.

To modify the communication port for Network Security Map

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the **Communication Port** box, type a new communication port number.
   You must use the same port number for each of the device that is connected to your **Network Security Map**.
4. Click **Apply**.
5. Click **OK**.

About Metered Broadband Mode

The Metered Broadband Mode feature lets you set up policies to restrict the Internet usage of Norton Internet Security. You can define the amount of network bandwidth that Norton Internet Security can use.

You can choose a communication policy that suits your Internet connection. If you have unlimited Internet plan, you can set up **No Limit** policy so that Norton Internet Security connects to Symantec servers to ensure complete protection. However, if you think that Norton Internet Security uses too much of your Internet connection, you can restrict the Internet usage of Norton Internet Security. Metered Broadband Mode helps you manage the data transfer between Norton Internet Security and your adapter.

To connect to the Internet, Norton Internet Security accesses the gateway through an adapter. The adapter is present either on your computer or on a connecting device. The connecting device can be a 3G phone, an Internet data card, or a wireless network card. Metered Broadband Mode lets you set up a policy for each adapter that Norton Internet Security uses to connect to the Internet.

You can set up one of the following policies for each of the adapter that Norton Internet Security uses to connect to the Internet:

- **No Limit**

  Lets Norton Internet Security use the network bandwidth that is required to ensure complete protection. Symantec recommends that you apply this policy.

- **Critical Updates Only**

  Lets Norton Internet Security access the Internet only to receive critical product updates or virus definitions. If you have a limited Internet connection, you can select the **Critical Updates Only** option to ensure protection from different security threats.

- **No Traffic**

  Lets you block Norton Internet Security from connecting to the Internet. If you choose this policy, Norton Internet Security cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.

Turning off or turning on Metered Broadband Mode

You can set up policies to restrict the Internet usage of Norton Internet Security. If you do not want to restrict the Internet usage of Norton Internet Security, you can turn off **Metered Broadband Mode**.

If you feel that Norton Internet Security uses too much network bandwidth, you can turn on **Metered Broadband Mode**. Then, you can set up policies to restrict the Internet usage of Norton Internet Security. Norton Internet Security connects to the Internet based on the policy that you set up in the **Metered Network Settings** window. By default, **Metered Broadband Mode** is turned on.

To turn off Metered Broadband Mode

1. In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Network Security Settings**.
4 In the **Metered Broadband Mode** row, move the **On/Off** switch to the right to the **Off** position.
5 Click **Apply**.
6 Click **OK**.

To turn on Metered Broadband Mode

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Network Security Settings**.
4 In the **Metered Broadband Mode** row, move the **On/Off** switch to the left to the **On** position.
5 Click **Apply**.
6 Click **OK**.

Defining the Internet usage of Norton Internet Security

If you think that Norton Internet Security uses too much of your network bandwidth, you can restrict the Internet usage of Norton Internet Security. You can set up policy for each adapter that Norton Internet Security uses to connect to the Internet.

The **Metered Network Settings** window lists all the adapters that your computer uses to connect the Internet. You can view the status of the adapters that are currently in use. The network policy that you set up defines the amount of network bandwidth that Norton Internet Security can use.

To define the Internet usage of Norton Internet Security

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Network Security Settings**.

4 In the **Metered Broadband Mode** row, move the **On/Off** switch to the left to the **On** position.

5 Click **Configure**.
The **Metered Network Settings** window lists all the adapters that Norton Internet Security uses to connect to the Internet.

6 Under the **Policy** column, click the drop-down list next to the adapter for which you want to set up a policy.

7 Select one of the following:

- **No Limit**

  Lets Norton Internet Security use the network bandwidth that is required to ensure complete protection.

- **Critical Updates Only**

  Lets Norton Internet Security access the Internet only to receive critical product updates or virus definitions.

  If you have a limited Internet connection, you can select the **Critical Updates Only** option to ensure protection from different security threats.

- **No Traffic**

  Lets you block Norton Internet Security from connecting to the Internet. If you choose this policy, Norton Internet Security cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.

8 Click **Apply**, and then click **OK**.

9 In the **Settings** window, click **OK**.

Securing your sensitive data

6

This chapter includes the following topics:

- About securing your sensitive data

About securing your sensitive data

The Internet provides the fastest and the easiest way to exchange information. In spite of the many advantages that the Internet provides, you are vulnerable to information theft and identity theft. Information can be stolen and misused in several ways.

Following are a few of the most common methods of information theft:

- Online financial transactions
- Unsafe online storage of sensitive information
- Misuse of your identity while you communicate online

The Identity Safe feature in Norton Internet Security offers several powerful ways to tackle identity theft. Identity Safe is the best tool that you can use to safeguard your identity while you are online.

About Safe Surfing

Safe Surfing comprises of the Antiphishing and the Norton Safe Web features. Antiphishing analyzes the security level of the Web sites that you visit and displays the results in the **Norton Site Safety** pop-up

window. The Norton Safe Web feature provides you a safe search environment in the Web by displaying the site rating icons next to every search result.

When you install Norton Internet Security, it adds the **Norton Toolbar** to the Internet Explorer, Firefox, or Chrome browsers. Norton Internet Security protects your Web browsers when you turn on the Antiphishing and Norton Safe Web options in the **Safe Surfing** section of the Norton Internet Security **Settings** window. The **Safe Surfing** section is available in the **Web** tab.

The Antiphishing and Norton Safe Web features are supported in the Internet Explorer, Firefox, or Chrome Web browsers.

When you turn off Antiphishing and Norton Safe Web features, Identity Safe may autofill fraudulent Web sites with your confidential information. Symantec recommends that you do not browse the Web when Antiphishing and Norton Safe Web features are turned off.

About Antiphishing

Antiphishing protects you from visiting unsafe Web sites. When Antiphishing is turned on, the Antiphishing component analyzes the security level of the Web sites that you visit. It then displays the results in the **Norton Site Safety** pop-up window. Antiphishing also blocks navigation to the Web sites that are confirmed to be fraudulent.

Antiphishing provides you the following information about the Web sites you visit:

- If the Web site is safe to enter confidential information
- If the Web site is fraudulent
- If the Web site is suspicious
- If the Web site is known to give annoying results

The **Norton Site Safety** pop-up window in Internet Explorer, Firefox, or Chrome Web browsers lets you view more details about the safety status of the Web sites you visit.

In addition, the **Norton Site Safety** pop-up window includes information about Symantec Authenticated Web sites. Web site hackers often mimic company Web sites to create fraudulent Web sites. Norton Internet Security identifies the fraudulent Web sites.

Symantec analyzes the pages of these sites and verifies if they belong to the company that it represents. You can be confident that the information that you provide goes to the company with which you want to do business.

You can report the evaluation of a Web site you suspect to be fraudulent to Symantec for further evaluation. Use the **Report Site** option from **Norton Toolbar** to report a Web site. You can also report the evaluation of a Web site that you suspect to be fraudulent but Antiphishing reports as safe.

Even when you turn off the **Antiphishing** option, Norton Internet Security protects you from Internet threats through its Norton Safe Web features. When Antiphishing is turned off, you cannot use the **Report Site** option in the **Norton** menu to submit the evaluation of the Web site to Symantec.

The **Norton Site Safety** pop-up window displays the following messages:

- **Site is Safe**
- **Site is Unsafe**
- **Site Untested**
- **Norton Secured**
- **Caution**
- **Fraudulent Site**
- **Suspicious Site**
- **Page Not Analyzed**

Reporting an incorrect evaluation of a Web site

On rare occasions, Antiphishing may report incorrect evaluation of a Web site. For example, you might visit a site that you shop with regularly and Antiphishing reports that the site is fraudulent. On the contrary, you might visit a Web site that you suspect is a phishing site, but Antiphishing reports that no fraud was detected. In either case, you can report the Web site to Symantec for further evaluation.

The Web site you want to report to Symantec for further evaluation must be kept open in your Web browser.

To report an incorrect evaluation of a suspicious Web site

1. Open your browser and go to the Web site that you think is suspicious.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Report site**.
3. In the dialog box that appears, verify that the Web site address and click **Submit**.
4. In the confirmation dialog box, click **Close**.

To report an incorrect evaluation of a safe Web site

1. Open your browser and go to the Web site that you think is safe.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Report site**.
3. In the dialog box that appears, verify that the Web site address and click **Submit**.
4. In the confirmation dialog box, click **Close**.

Turning off or turning on Antiphishing

Antiphishing protects you from visiting unsafe Web sites. The Antiphishing feature in Norton Internet Security analyzes the security level of all the Web sites that you visit and displays the results in the **Norton Site Safety** pop-up window. Antiphishing also blocks

navigation to the Web sites that are confirmed to be fraudulent.

The **Norton Site Safety** pop-up window helps you understand if the Web site that you visit is safe or unsafe.

You can turn off or turn on Antiphishing in the **Safe Surfing** section of the **Settings** window. The **Safe Surfing** section is available in the **Web** tab.

To turn off or turn on Antiphishing

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Safe Surfing**.
4. In the **Antiphishing** row, do one of the following:
   - To turn off Antiphishing, in the **Antiphishing** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Antiphishing, in the **Antiphishing** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

About Norton Safe Web

Norton Safe Web helps you surf, search, and shop more safely on the Internet. By using Norton Safe Web, you can check if a Web site is malicious or not even before you visit it. Norton Safe Web analyzes the Web sites you visit and detects if there are any viruses, spyware, malware, or other security threats that exist on the Web sites. Based on the analysis, Norton Safe Web provides safety ratings for all the Web sites.

In addition, Norton Safe Web lets you view the community rating and user reviews of the Web sites you visit.

Norton Safe Web supports Internet Explorer, Firefox, or Chrome Web browsers.

You can view the site safety status of any Web site using the **Full Report** option on the **Norton Site Safety** pop-up window. You can also use the **Community Buzz** option on the **Norton** menu to view the safety status of the Web sites.

The **Community Buzz** option is available only in English-language versions of Windows.

For each Web site that you want to know the site safety status, Norton Safe Web lets you do the following:

- View the Norton rating.
- View the community rating.
- Add your reviews.
- View the user reviews.
- View a list of keywords that are tagged to the Web site.
- View the threat information and the general information about the Web site.

If you use a proxy server to connect to the Internet, you must configure the Network Proxy Settings of Norton Internet Security.

When you search the Internet using Google, Yahoo, or Bing search engines, Norton Safe Web displays site rating icons next to the search results. As you move the mouse pointer over an icon, a pop-up appears with site safety and shopping safety information. The pop-up displays brief information about the safety of the site. Norton Safe Web also provides a detailed report about the safety of the Web Sites you visit.

You can click the icon next to the search results or the **Full Report** option in the **Norton Site Safety** pop-up window to view the detailed report. The report is displayed on the Norton Safe Web site.

Norton Safe Web provides the following Web site safety states when you browse through the Internet:

Norton Secured	You can see Norton Secured icon next to the search results. Symantec has analyzed this page and determined that the Web site is VeriSign trusted and is safe to visit.
Site is Safe	You can see a green OK icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that it is safe to visit.
Site Untested	You can see a gray question mark icon next to the search results. When you visit this Web site, the **Norton Toolbar** shows a green OK icon. Norton Safe Web has not analyzed this Web site and it does not have sufficient information about this web site. As Symantec has not tested the Web site, it is recommended that you do not visit this Webs site.

Site is Unsafe	You can see a red cross (x) icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that the Web site is unsafe to visit. This Web site may attempt to install malicious software on your computer.
Caution	You can see a yellow exclamation mark icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that this web site has some threats that are classified as **Annoyance Factors**. These annoyance factors are not dangerous, but it can install unwanted applications on your computer without your permission.

In addition to the site safety information, Norton Safe Web provides the following shopping safety information:

Safe	Norton Safe Web has analyzed this Web site and determined that you can have a safe shopping experience.

Untested	Norton Safe Web does not have sufficient information about this Web site to provide a shopping safety rating.
Risky	Norton Safe Web has analyzed this Web site and determined that the site has shopping risks. Symantec recommends that you do not visit this page. The Web site may sell counterfeit items without proper indication.
Limited	Norton Safe Web has analyzed this Web site and has only some information about the Web site to provide shopping safety information. The information is not sufficient to declare that the Web site is safe to shop.

When you visit any Web site that has an unsafe status, Norton Safe Web blocks that Web page. If you still want to view the Web site, use the **Continue to site anyway** option that appears on the blocked page. You can use the **Block Malicious Pages** option to block malicious pages. To access the **Block Malicious Pages** option, go to the Norton Internet Securitymain window, and then click **Settings > Web > Safe Surfing > Block Malicious Pages**. If you turn off the **Block Malicious Pages** option, Norton Safe Web does not block the unsafe Web sites. However, **Norton Toolbar** displays the status of these Web sites as unsafe even when the option is turned off.

In addition, Norton Safe Web protects your computer while you use Facebook. It scans each URL that is available on your Facebook Wall and displays the Norton rating icons for the scanned URLs. You can also

let other Facebook users know about the security status of any Web site.

To scan your Facebook Wall using Norton Safe Web, use the **Scan Facebook Wall** option. The option appears when you click the **Scan Now** option in the Norton Internet Security main window.

Searching the Web using Norton Safe Search

Norton Safe Search enhances your Web search experience. When you search the Internet using Norton Safe Search, it uses Ask.com to generate the search results. Norton Safe Search provides the site safety status and Norton rating for each of the search results generated.

By default, the **Norton Safe Search** box is disabled. After you install Norton Internet Security and open Internet Explorer, Firefox, or Chrome Web browsers for the first time, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search.

Norton Safe Search provides you the intelligent search-as-you-type feature that displays search suggestions when you type a few letters of the search phrase.

In addition, Norton Safe Search provides the following features:

Unsafe Site Filter	When you search the Internet using Norton Safe Search, it analyzes the security levels of the Web sites and displays the search results. You can use the **Filter Out Unsafe Sites** option in the Norton Safe Search Web site to filter the unsafe Web sites from the search results. When you click the **Filter Out Unsafe Sites** option the **Unsafe Site Filter** option is turned on. By default this option is turned off.
Erase Search History	Norton Safe Search enables you to erase all the data that are related to your search activities from the Ask.com server. The Privacy Safeguard feature of Norton Safe Search removes the search data, such as your IP address, user identifier, and session identifier from the Ask.com server. You can turn on or turn off Privacy Safeguard using the **Turn On Privacy Safeguard** and **Turn Off Privacy Safeguard** options respectively.

Norton Safe Search feature is available only for some regions including the United States, the United Kingdom, Canada, Australia, and Germany. The Privacy Safeguard feature is available only for the United States, the United Kingdom, and Canada.

You can use Norton Safe Search even when you turn off the Identity Safe features.

Norton Safe Search is supported only by the Internet Explorer, Firefox, or Chrome Web browsers.

To search the Web using Norton Safe Search

1. Start your Web browser.
2. On the **Norton Toolbar**, in the **Norton Safe Search** box, type the search string that you want to search.
3. Do one of the following:
   - Click **Search**.
   - In the pop-up window that appears, select a search suggestion that matches your search string.

Turning off or turning on Norton Safe Web

Norton Safe Web protects your computer while you browse the Internet using Internet Explorer, Firefox, or Chrome Web browsers. It analyzes the security levels of the Web sites that you visit and indicates if the Web sites are free from threats. It provides you a safe environment on the Web by displaying the site rating icons next to each search result. The site rating icons lets you know if a Web site is malicious or not even before you visit it.

You can turn off or turn on Norton Safe Web in the **Safe Surfing** section of the **Settings** window.

To turn off or turn on Norton Safe Web

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Safe Surfing**.

4 In the **Norton Safe Web** row, do one of the following:
   - To turn off Norton Safe Web, in the **Norton Safe Web** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Norton Safe Web, in the **Norton Safe Web** row, move the **On/Off** switch to the left to the **On** position.
5 In the **Settings** window, click **Apply**.
6 Click **OK**.

About Identity Safe

Identity Safe helps you manage your identities and provides additional security while you perform online transactions.

The following features in Identity Safe provide secure storage of your sensitive information:

Edit Logins	Stores login information, such as your login credentials for your online bank account, email user ID, and password.
Edit Identity Cards	Stores your personal information, such as addresses, date of birth, and credit card information.
Edit Notes	Stores the details, such as passport numbers and social security numbers.

In addition to being a depository of sensitive information, Identity Safe provides the following features:

- Protects you from identity theft when you perform online transactions

Antiphishing also helps to protect you from malicious Web sites when you perform online transactions.

- Manages your card information when you have multiple credit cards to maintain
- Safeguards the data that you save on your computer

  By saving your data with a local vault, you can prevent your sensitive Identity Safe data on your computer from being misused. A local vault is specific to each of the Windows user accounts present on your computer.
- Provides you the ease of carrying and using your Identity Safe data when you are on the move

  By saving your data using an online vault, you can access your sensitive Identity Safe data from any computer that has Norton Internet Security installed.

Norton Internet Security adds the **Norton Toolbar** to the Internet Explorer, Firefox, or Chrome Web browsers. The **Norton Toolbar** has the following components:

- **Norton** menu
- **Norton Safe Search**
- **Safe Web** indicator
- **Identity Safe** menu

When you have cards or logins in Identity Safe, the **Identity Safe** menu displays the list of cards and logins.

Norton Internet Security supports Google Chrome version 10.0 or later.

If you turn off Identity Safe, you cannot access your logins and Identity Safe features from the **Norton Toolbar**.

Norton Internet Security lets you view and access some of the Identity Safe features even after the product expires. This way, you can still view your login details even after Norton Internet Security expires. However, it is not safe to browse the Internet after Norton

Internet Security expires as you are vulnerable to online thefts and phishing attacks.

The following are the activities that you can perform after the product expires:

- Back up your Identity Safe data and save it as a .DAT or .CSV files.
- Open the **Edit Logins** window and view the logins that you saved.

About setting up Identity Safe

Identity Safe helps you manage your sensitive information and provide additional security while you perform online transactions. The features in Identity Safe provide a secure storage for your personal information such as your address, login information, passwords, and credit card details.

Identity Safe provides a secure storage for the following:

- Login information such as user IDs and passwords of your email accounts
- Personal information such as your address, date of birth, passport number, and social security number.
- Credit card details including card number and card expiry date.

You can view all the options that are available in Identity Safe only after you set up Identity Safe.

For each Windows user account, Identity Safe lets you create a local vault and save your Identity Safe data. The data that you save and any of the Identity Safe settings that you configure are specific to that local vault. You cannot access the data that you save in one Windows user account from another user account. This way Identity Safe protects your sensitive data from being misused even when you share your computer with others.

In addition to the local vault that you create on a Windows user account, you can also save your Identity Safe data in online vault.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton Internet Security must be installed.
- The computer must be connected to the Internet.

The Identity Safe data is stored online using your Norton Account. You can create only one online vault for a Norton Account.

If you have Identity Safe data that is stored on any external drives from the older versions of Norton Internet Security, you can convert that portable profile to local vault or online vault. When you connect your external drive to your computer, the Identity Safe menu in the **Norton Toolbar** provides option to merge or delete the Identity Safe data from your portable profile. You can merge the data from the portable profile to local vault or online vault.

Turning off or turning on Identity Safe

Identity Safe helps you manage your identity and provides additional security while you perform online transactions. You can use the various features in Identity Safe to manage your personal data such as addresses, date of birth and credit card information. The logins, cards, and notes help you store and use your personal information in a secure way.

After you turn on Identity Safe, you must log in to Identity Safe to access the various features.

To turn off or turn on Identity Safe from Settings window

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.

4 In the **Identity Safe** row, do one of the following:
   - To turn off Identity Safe, in the **Identity Safe** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Identity Safe, in the **Identity Safe** row, move the **On/Off** switch to the left to the **On** position.
5 In the **Settings** window, click **Apply**.
6 Click **OK**.

About Identity Safe vaults

You can create one local vault for each Windows user account on your computer. The data that you save and the Identity Safe settings that you make are specific to that local vault. You cannot access the data that you save in one Windows user account from another Windows user account. This way Identity Safe protects your sensitive data from misuse by multiple users of your computer.

Symantec recommends that you create separate password-protected Windows user accounts if you want to share your computer with multiple users.

In addition to the local vault that you create on a Windows user account, you can save your Identity Safe data in online vault. When you move your Identity Safe data from local vault to online vault, the data in your local vault is permanently removed. The Identity Safe data is stored online using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton Internet Security must be installed.
- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account.

If you have Identity Safe data that is stored on any external drives from the older versions of Norton Internet Security, you can convert that portable profile to local vault or online vault. When you connect your external drive to your computer, the **Identity Safe** menu in the **Norton Toolbar** provides option to merge the Identity Safe data from your portable profile. You can merge the data from the portable profile to your local vault or online vault.

In addition to the features such as saving logins, cards, and notes, you can do the following using your Identity Safe vault:

- Import your Identity Safe data from the file you already backed up. You can also import the data that you stored in portable profile from an older version of the product to the current version.
- Export your Identity Safe data to .DAT file.
- Reset your Identity Safe.

About creating Identity Safe vaults

Identity Safe helps you manage your sensitive information and provide additional security while you perform online transactions. The various features in Identity Safe provide a secure storage for your personal information such as your address, login information, passwords, and credit card details.

Identity Safe lets you create one local vault per Windows user account.

In addition to the local vault, you can save your Identity Safe data in online vault. When you move your Identity Safe data from local vault to online vault, the data in your local vault is permanently removed.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton Internet Security must be installed.

- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account. You must log in to your Norton Account to move Identity Safe data from the local vault to the online vault.

You can create Identity Safe vaults from the **Identity Safe** section of the **Settings** window. The **Identity Safe** section is available in the **Web** tab.

Creating local vault and online vault

Identity Safe lets you create a local vault and save your Identity Safe data. You can create one local vault for each Windows user account.

In addition to the local vault that you create on a Windows user account, you can also save your Identity Safe data in online vault. The Identity Safe data is stored online vault using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton Internet Security must be installed.
- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account.

To create local vault

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
5. In the **Set Up Identity Safe** window, in the **Create Password** box, type your password.
6. In the **Confirm Password** box, type the password again to confirm.

7 In the **Password Hint** box, type a hint for the password.
8 Uncheck the **Store information online through your Norton Account** checkbox.
This option appears only if you log in to your Norton Account. By default, this option is checked.
9 Click **Create**.
10 In the **Identity Safe Setup Successful** window, click **Done**.

To create online vault

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
5 In the **Set Up Identity Safe** window, in the Create Password box, type the password.
You must provide a strong password to create online vault. You can click **How to create a strong password?** link to know more about creating strong passwords.
6 In the **Confirm Password** box, type the password again to confirm.
7 In the **Password Hint** box, type a hint for the password.
8 Check the **Store information online through your Norton Account** checkbox.
This option appears only if you log in to your Norton Account.
9 Click **Create**.
10 In the **Identity Safe Setup Successful** window, click **Done**.

Logging in to Norton Account

Identity Safe lets you create a local vault and an online vault to save your Identity Safe data. You must log in

to your Norton Account to create an online vault. The Identity Safe data is stored online using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton Internet Security must be installed.
- The computer must be connected to the Internet.

You can create only one online vault per Norton Account. If you already have a Norton Account, you can log in with your credentials or create a new account.

To log in to Norton Account

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
5. At the bottom of the **Set Up Identity Safe** window, click **Login**.
6. In the **Login to Norton Account** window, type your **E-mail Address** and **Password**.
7. Click **Log In**.

Moving local vault to online vault

You can move the Identity Safe data from your local vault to the online vault. When you move the data from your local vault to online vault, all the data in your local vault is removed permanently.

The **Move Identity Safe Online** option in Identity Safe helps you to save your data online.

The following are the benefits of moving your Identity Safe data online:

- Lets you access you Identity Safe data from any computer.

  Your computer must have the latest version Norton Internet Security installed and must be connected to the Internet.

- Lets you access your Identity Safe data from online vault without depending on any external drive.
- Provides a convenient means to automatically synchronize Identity Safe data across different computers using your Norton Account.

You must log in to your Norton Account to move the Identity Safe data from your local vault to online vault.

To move local vault to online vault

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Move Identity Safe Online** row, click **Configure**.
5. In the **Move Identity Safe Data Online** window, in the **Enter the Password** box, type the password for your local vault.
6. Click **Login**.
   If you have provided a password of poor strength while creating the local vault, Identity Safe prompts you to provide strong password before you move the data from local vault to online vault.
7. In the **Move Identity Safe Data Online** window, click **Move Vault**.
8. In the confirmation dialog box, click **Yes**.
9. In the **Move Identity Safe Data Online** window, click **Done**.

Deleting local vault and online vault

Identity Safe lets you create a local vault and an online vault to save your Identity Safe data. If you no longer

require your Identity Safe data that is stored in your local vault and online vault, you can delete the vaults. When you delete the local vault and online vault, all the Identity Safe data is permanently removed.

To delete the local vault and online vault

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Delete Identity Safe** row, click **Configure**.
5. In the **Warning** window, click **Yes**.
6. In the **Settings** window, click **Apply**.
7. Click **OK**.

Merging portable profile to local vault or online vault

If you have Identity Safe data that is stored on any external drives from the older versions of Norton Internet Security, you can merge that portable profile to local vault or online vault. When you connect your external drive to your computer, the **Identity Safe** menu in the **Norton Toolbar** provides option to merge the Identity Safe data from your portable profile. You can merge the data from the portable profile to local vault or online vault.

You can merge the Identity Safe data from the portable profile to the vault that you are currently logged in.

To merge the Identity Safe data from portable profile to local vault or online vault

1. On the **Norton Toolbar**, in the **Identity Safe** menu, Click **Merge Portable Data (Drive:\)** .
   This option appears only if you connect an external drive with portable profile.
2. In the dialog box that appears, click **Yes**.
3. In the **Import Identity Safe Data** window, under **Import my data from**, click **Portable Profile (Drive:\)**.

4 In the **Password** box, type the password.
5 Do one of the following:
- If you want to delete the data from the portable profile after import, check **Delete original data once merged**.
- If you do not want to delete the data from the portable profile after import, uncheck **Delete original data once merged**.

Importing logins

Identity Safe lets you import the logins that you have saved in Internet Explorer. After you set up Identity Safe vaults, the **Identity Safe Setup Successful** window appears.

You can use this window to import your logins. The imported logins appear in the **Identity Safe** menu on the **Norton Toolbar** and in the **Edit Logins** window. You can use the imported logins the same way that you use the logins that you create.

To import logins

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
5 Set up Identity Safe.
6 In the **Identity Safe Setup Successful** window, do one of the following:
- Check **Import my logins from Internet Explorer** checkbox to import all the logins that you saved in your Web browser.
- Uncheck **Import my logins from Internet Explorer** checkbox, if you do not want to import all the logins that you saved in your Web browser.

7 In the **Identity Safe Setup Successful** window, click **Done**.

Resetting Identity Safe

There may be instances when you need to reset your Identity Safe.

You may need to reset your Identity Safe in the following occasions:

- You experience a computer failure.
- You forget your Identity Safe password.

If you forget your Identity Safe password, you cannot restore it. You can only reset your Identity Safe and store all your data again.

Norton Internet Security lets you enter an incorrect password three times. If your attempts are unsuccessful, Norton Internet Security provides you an option to reset your Identity Safe. If you reset the Identity Safe, you lose all the Identity Safe data that you stored, such as your login information, cards, and notes.

To reset your Identity Safe

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Log in to Identity Safe** row, click **Configure**.
5 In the **Enter the Password** box, type your **Identity Safe** password.
If you forget your password, Identity Safe lets you enter wrong password three times. If your attempts are unsuccessful, the **Trouble Logging In?** window appears.

6 In the **Trouble Logging In?** window, click **Reset Identity Safe**.
If you forget the Identity Safe password of your online vault, you need to provide your Norton Account credentials to reset your Identity Safe.

7 In the confirmation dialog box, click **Yes**.

Accessing Identity Safe

You can access the Identity Safe settings from the following sections of Norton Internet Security:

- From the **Web** tab in the Norton Internet Security **Settings** window
- From the **Norton Toolbar**

With Norton Internet Security, you can access and configure some of the Identity Safe features even after the product expires. The following are the features that you can view or access after the product expires:

Edit Logins	You can view the **Edit Logins** window using the **Identity Safe** menu on the **Norton Toolbar**. Although the product is expired, you can still view all the logins that you saved for a Web site. However, you cannot save, add, or update that logins after the product expires.
Export Identity Safe data	You can use this feature to take a backup of your Identity Safe data. The data that you back up are stored as .DAT file.

You must be logged in to Identity Safe to access the Identity Safe features. The Identity Safe features are supported only by the Internet Explorer, Firefox, or Chrome Web browsers.

To access Identity Safe settings from the main window

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, for the Identity Safe feature that you want to open, click **Configure**.

To access Identity Safe settings from the Norton Toolbar

1. Start your Web browser.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Settings**.
3. For the Identity Safe feature that you want to open, click **Configure**.

Logging in to and logging out of Identity Safe

You can log in to or log out of Identity Safe from the following areas of Norton Internet Security:

- The **Web** tab in the Norton Internet Security **Settings** window
- The Norton Toolbar

To secure your Identity Safe data from others, log out of Identity Safe whenever you are away from your computer.

Identity Safe automatically logs you out of the current vault, when you are logged in to your local vault or online vault and click **Identity Safe Setup** to create a new vault

To log in to Identity Safe

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Log in to Identity Safe** row, click **Configure**.

5 In the **Log in to Identity Safe** window, in the **Enter the Password** box, type the password of the vault you want to log in.
6 Click **Login**.

To log out of Identity Safe

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Log out of Identity Safe** row, click **Log out now**.

To log in to Identity Safe from the Norton Toolbar

1 Start your Web browser.
2 On the **Norton Toolbar**, click **Identity Safe**.
3 In the **Log in to Identity Safe** window, in the **Enter the Password** box, type the password of the vault you want to log in.
4 Click **Login**.

To log out of Identity Safe from the Norton Toolbar

1 Start your Web browser.
2 On the **Norton Toolbar**, click **Identity Safe**, and then click **Log out of Identity Safe**.

Configuring Identity Safe settings

You can use the various features in Identity Safe to manage your personal sensitive information. The logins, cards, and notes help you store and use your information in a secure way.

To configure Identity Safe settings

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.

4 Under **Identity Safe**, identify the feature that you want to use, and click **Configure**. Your options are:

Identity Safe Setup	Lets you set up Identity Safe vault. You can create a local vault or an online vault and store your Identity Safe data. You must log in to your Norton Account to create an online vault.
Export Identity Safe Data	Lets you back up the Identity Safe data in .DAT or .CSV file formats. You should back up all of your Identity Safe data periodically.
Move Identity Safe Online	Lets you move your Identity Safe data that you stored in your local vault to online vault. When you move your Identity Safe data from local vault to online vault, the data in the local vault is permanently removed.
Delete Identity Safe	Lets you permanently remove the Identity Safe vault.

Identity Safe Options	Lets you set the options that let Identity Safe securely collect and store your Web page login information. In addition, you can do the following activities: ▪ Configure the region for your card information. ▪ Specify how you want Norton Identity Safe to use the autofill feature. ▪ Set the options that make Identity Safe to display a message to notify you that you have inserted an external drive. ▪ Set the options that make Identity Safe to warn you about the unsafe removal of external drives.
Identity Safe Password & Security	Lets you change the password settings and the security level of your Identity Safe password. You should change your Identity Safe password frequently to keep your Identity Safe data from being misused.

Edit Identity Cards	Lets you manage your personal information such as name, date of birth, email address, and credit card information in one place. You can use the information that you store to automatically fill forms. This feature lets you provide sensitive information without typing it when you are online. In this way, Identity Safe protects you from keyloggers that steal and misuse your identity.
Edit Logins	Lets you manage your various login information. Logins include information such as your email login credentials and Internet banking credentials. When you save all of your login information in the Identity Safe, you can do the following: ▪ Easily track all your logins ▪ Quickly launch your login Web sites ▪ View or update your password for the Web site ▪ Use folders to organize your logins ▪ Change your login settings

Edit Notes	Lets you store and manage sensitive information. You can save social security number, driver's license number, insurance policy number, and passport number. You can also save private accounts, lock combinations, documents, notes, frequent flier numbers, bank account number, security challenge questions, and legal and financial information.
Import Identity Safe Data	Lets you import the Identity Safe data from the backed up file or from the portable profile that you have from the older versions of Norton Internet Security. When you import the Identity Safe data you have the following options: ▪ Merge the imported data in to the vault that you are currently logged in. ▪ Replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

About Edit logins

The Edit Logins feature in Identity Safe lets you view all the logins that you want Identity Safe to manage. Login information includes information such as your email login credentials and Internet banking credentials.

Identity Safe provides you the option to save your logins when you enter your login information in a Web

site's login page. You can instantly save your login information in Identity Safe.

To manage your logins, you must be logged in to Identity Safe.

Identity Safe offers the following features:

- Safely stores Web site login information
- Lets you save multiple IDs or accounts and passwords for a Web site
- Lets you organize your logins under various folders
- Intelligently searches for a particular login
- Lets you save the Web site name with a name other than the default name
- Displays the login ID and lets you show or hide the password
- Displays the strength of the password for your login
- Lets you quickly launch the Web site login page
- Fills in your login automatically when you revisit Web pages
- Lets you manually add logins
- Lets you change the URL of your saved logins
- Lets you view the last time you made changes to the settings of your saved logins
- Lets you view and fill the login details that you saved for a Web site even after Norton Internet Security expires. To do so, use the **Identity Safe** menu on the **Norton Toolbar** in the Web browser.

The Identity Safe features are supported in the Internet Explorer, Firefox, or Chrome Web browsers.

Norton Internet Security supports Google Chrome version 10.0 or later.

Saving logins

Identity Safe lets you save your logins when you log in to a Web site for the first time. You can save multiple

logins for the same Web site. You can also save the same login for different Web sites.

When you provide your login credentials on a Web site, Identity Safe displays **Save your login for this site?** on the **Norton Toolbar**. You can provide a name for your login and select the folder in which you want to save your login. The folders that you create appear in the **Folder** drop-down list in the **Save login for site** dialog box.

After Identity Safe saves a login, it automatically fills the login details next time you visit the Web site.

You must be logged in to Identity Safe to save and use autofill passwords. If the password or user name field is blank, Identity Safe does not prompt you to save the login.

Identity Safe lets you view and fill the login information that you saved for a Web site even after the product expires. You can use the **Identity Safe** menu on the **Norton Toolbar** to view the logins.

You can only view your saved logins after Norton Internet Security expires, you cannot save or add any new logins.

When you try to save a login after the product expires, a pop-up window appears and suggests you to renew the subscription of the product. You can use the pop-up to renew the subscription.

To save a login

1. Go to the Web site for which you want to save your login.
2. Type your login details, and then click the option or link that logs you in.

3 On the **Norton Toolbar**, in the **Save your login for this site?** row, do one of the following:
   - If you want to save your login, click **Save**. In the **Save Login for Site** dialog box, type a name for your login in the **Name** box, select the folder in which you want to save your login from the **Folder** drop-down list, and then click **Save**.
   - If you do not want to save your login this time, click **Don't Save**.
   - If you never want to save your login, click **Never**.

To save additional logins for a Web site

1 Go to the Web page for which you want to save another login.
   Your login credentials automatically appear on the Web page.
2 Clear the login credentials that appear on the Web page.
3 Type the new login, and then click the option or link that logs you in.
4 On the **Norton Toolbar**, in the **Save your login for this site?** row, click **Save**.
5 In the **Save Login for Site** dialog box, type a name for your login in the **Name** box, select the folder in which you want to save your login from the **Folder** drop-down list.
6 Click **Save**.

Editing logins

Edit Logins lets you view all of the logins that you want Identity Safe to manage.

Edit Logins provides the following features:

- Lets you safely store Web site login information.
- Lets you save multiple IDs or accounts and passwords for a Web site.
- Lets you organize your logins under various folders.
- Intelligently searches for a particular login.

- Lets you save the Web site name with a name other than the default name.
- Displays the login ID and lets you show or hide the password.
- Displays the strength of the password for each of the logins.
- Lets you quickly launch the Web site login page.
- Fills in your login automatically when you revisit Web pages.
- Lets you manually add logins.
- Lets you change the URL of your saved logins.
- Lets you view the last time you made changes to the settings of your saved logins.

Edit Logins also lets you view and fill the login details that you saved for a Web site even after Norton Internet Security expires. To do so, use the Identity Safe menu on the **Norton Toolbar**.

To create a new folder

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5. In the **Edit Logins** window, click **Create New Folder**.
6. In the **New Folder** dialog box, in the **Enter new folder name** box, type a folder name.
7. Click **OK**.
8. Click **Close**.
9. In the **Settings** window, click **OK**.

To add a login manually

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.

4 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5 In the **Edit Logins** window, click **Create New Login**.
6 In the **New Login** dialog box, type the URL of the Web site or a name for which you want to use this login.
If it is a URL, ensure that you prefix it with HTTP.
7 Click **OK**.
8 In the **Username** dialog box, in the **Enter new username** box, type the user name of the login, and then, click **OK**.
9 In the **Information** dialog box, click **OK**.
The **Information** dialog box prompts you to set a password for the login that you created.
10 In the **Edit logins** window, in the **Password** box, type the password of your login.
11 Click **Close**.
12 In the **Save** dialog box, click **Yes** to save the changes.
The **Save** dialog box appears only if you set a password for the login that you created.
13 In the **Settings** window, click **OK**.

To set a password for the login that you added manually

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5 In the **Edit Logins** window, under **Logins**, select the login for which you want to set a password.
6 Under **Details**, next to **Password** box, click **Show**.
The **Validate Password for Identity Safe** window appears. This window appears only if you have changed the Identity Safe password security level to **Ask for my password before filling out a Login** in the **Password & Security** window.

7 In the **Validate Password for Identity Safe** window, do the following:
   - In the **Enter the Password** box, type your Identity Safe password.
   - Click **Login**.
8 In the **Edit Logins** window, in the **Password** box, type your Identity Safe password.
9 Click **Close**.
10 In the confirmation dialog box, click **Yes** to save the changes.
11 In the **Settings** window, click **OK**.

To delete a login or a folder

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5 In the **Edit Logins** window, under **Logins**, select the Web site name or the folder that you want to delete.
6 Click **Delete**.
7 In the confirmation dialog box, click **OK**.
8 Click **Close**.
9 In the **Settings** window, click **OK**.

Managing your URL details

Edit Logins lets you view the URL of the logins that you saved. You can view the URL of the Web site logins that you save in Edit Logins.

When you save a login, you can do the following:

- Quickly launch the Web site login page using the URL
- Change the URL of the login manually

  Ensure that the URL you change belongs to the same domain as the current URL.

- View the details of the date and time when you last made to the Edit Logins settings

To quick-launch a login Web page

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5. In the **Edit Logins** window, under **Logins**, select the login for which you want to launch the Web site.
   If you have saved your login in a folder, double-click the folder and select the login.
6. Under **Details**, click the URL that is available next to the **Address** option to launch the Web site.
7. Click **Close**.
8. In the **Settings** window, click **OK**.

To change the URL of your login

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5. In the **Edit Logins** window, under **Logins**, select the login for which you want to launch the Web site.
6. Under **Details**, click **Change** that is available next to the **Address** option.
7. In the **Update URL** window, in the **Enter the new URL here** box, type the new URL.
   Ensure that the URL you modify is valid and is prefixed with HTTP.
8. Click **OK**.
9. In the **Edit Logins** window, click **Close**.
10. In the **Settings** window, click **OK**.

Changing the user name and password

Identity Safe lets you change the user name and password for the logins that you have saved in the **Edit Logins** window. The updated information is automatically filled the next time you visit that Web page.

To change the user name

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5. In the **Edit Logins** window, under **Logins**, select the Web site name for which you want to change the user name.
6. Under **Details**, next to **Username** box, click **Change**.
7. In the **Username** dialog box, in the **Enter new username** box, type the new user name.
8. Click **OK**.
9. In the **Edit Logins** window, click **Close**.
10. In the **Settings** window, click **OK**.

To change the password

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
5. In the **Edit Logins** window, under **Logins**, select the Web site name for which you want to change the password.

6 Under **Details**, next to the **Password** box, click **Show**.
The **Validate Password for Identity Safe** window appears. This window appears only if you have changed the security level of the Identity Safe password to **Ask for my password before filling out a Login** in the **Password & Security** window.

7 In the **Validate Password for Identity Safe** window do the following:

- In the **Enter the Password** box, type your Identity Safe password.
- Click **Login**.

8 In the **Edit Logins** window, in the **Password** box, type the new password.

9 Click **Close**.

10 In the confirmation dialog box, click **Yes** to save the changes.

11 In the **Settings** window, click **OK**.

Updating the password for a login

Good security practice requires that you regularly change the password for a login. You can keep your login credentials in Identity Safe updated every time you change your password for a Web page. The updated information is automatically filled the next time you visit that login's associated Web page.

You can also update your new login information in Identity Safe when you are on the Web page. Identity Safe asks you if you want to update your logins.

To update the password for a login

1 Go to the Web page for which you want to change the password information.

2 Clear the password entry that Identity Safe autofilled.

3 Type the new password, and then click the button or link that logs you in.

4 In the **Save new password for login?** menu bar, click **Save**.

About Edit Identity Cards

The **Edit Identity Cards** option in Identity Safe lets you manage your personal information such as name, date of birth, email address, and credit card information in one place.

You can use the information that you store in the cards to do the following:

- Automatically fill forms
- Provide sensitive information without having to type it while you are online

In this way, Identity Safe protects you from keyloggers that steal and misuse your identity.

Some Web sites have forms with fields for credit cards or other personal information. The **Identity Safe** menu on the **Norton Toolbar** lists the cards that you created for autofill. You can choose a card from the list to fill the forms automatically.

You can add, view, edit, and duplicate the details of any card that you create. You can also delete a card if it is no longer needed.

In addition, Edit Identity Cards provides you the following features:

- Lets you password-protect the card to protect yourself from misuse of your sensitive information and personal information
- Recognizes the Web pages that have forms and immediately displays a pop-up window with the list of cards
- Provides you a quick view of any of your cards that is not password-protected

  Identity Safe provides additional security for your password-protected cards by not displaying the summary of the card

When you are on a Web page that has forms, the **Fill fields on this page?** menu bar in the **Norton Toolbar** displays the cards that you saved. You can click the **Fill Form** option in the **Fill fields on this page?** menu bar and select the card that you want to use to fill the Web site. You can also use the **Fill with Identity Card** option in **Identity Safe** menu to select the cards.

Adding cards

The cards in the **Edit Identity Cards** window help you to automatically fill forms on Web sites with a single click. You can create cards to store information, such as personal details, contact details, and credit card details. You can provide a card name to help you identify a specific card.

If you have more than one credit card, you can create multiple cards with different sets of information. When you visit a transactional Web site, you can provide the credit card details that are present in any of the cards that you created.

You can also create anonymous cards for use on unfamiliar Web sites where you may be uncomfortable providing your personal information. You can automatically fill online forms when you visit a Web site.

To add a card

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Identity Cards** row, click **Configure**.
5. In the **Edit Identity Cards** window, click **Add Card**.

6 Use the following tabs to type your card details:

General	Provide details such as card name, name, gender, and date of birth. You can set a password and provide additional security for your card. Online form filling is language-specific. In the **Country/Region** box, the country United States is selected by default. You should change your region and create a new card before you fill online forms for any other language.
Contact	Provide your contact information in this section. . Contact information includes your email address, postal address, and phone numbers.
Credit Card	Provide your credit card details such as the type of the card, expiration date, and card number in this section. You cannot enter a credit card number of more than 16 digits.

7 Click **Save**.

8 Click **Close**.

Editing, deleting, or duplicating cards

All the cards that you have saved in Identity Safe are listed in the **Edit Identity Cards** window. You can select, view, duplicate, and edit the details of any card that you created. You can delete a card if it is no longer needed. You can also duplicate a saved card and change only the fields that you want to change.

You can view a summary of the card that you created. You can select any of the cards that are present in the list of cards at the bottom of the **Edit Identity Cards** window. When you select a card, you can view a summary of the card.

When you lock your card with a password, Identity Safe provides additional security to your card. You cannot view the summary of the locked card. You cannot edit, delete, or duplicate a card unless you provide the password.

If you have multiple cards, use the scroll arrows to browse the list.

When you create, duplicate, or edit a card, the card's region is set to the user's default region. If you browse to a Web site other than the default region and use the card to fill the form on that Web site, the fields may not fill correctly. For example, your card has a default United States region but you are on a France Web page. In this case, you must use the card with France as the region to fill the Web page form.

To edit a card

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Identity Cards** row, click **Configure**.
5. In the **Edit Identity Cards** window, select the card that you want to edit.
6. Click **Edit Card**.
7. Modify the required details that you want to change..
8. Click **Save**.
9. Click **Close**.

To delete a card

1. In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Edit Identity Cards** row, click **Configure**.
5 In the **Edit Identity Cards** window, select the card that you want to delete.
6 Click **Delete Card**.
7 In the confirmation dialog box, click **OK**.
8 Click **Close**.

To duplicate a card

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Edit Identity Cards** row, click **Configure**.
5 In the **Edit Identity Cards** window, select the card that you want to duplicate.
6 Click **Duplicate Card**.
7 Modify the details that you want to change.
8 Click **Save**.
9 Click **Close**.

About Edit Notes

Identity Safe stores and manages your sensitive information. It becomes difficult to manage all of the identity numbers that you use when you browse the Web. The **Edit Notes** option in Identity Safe stores all your sensitive IDs in a very secure way and lets you use them easily when you are online. You can use Edit Notes to save information such as social security number, driver's license number, insurance policy number, and legal and financial information.

Editing Notes

You can use the **Edit Notes** option in Identity Safe to store your personal information, which you can retrieve and use when needed. You can use this information to fill out Web site registration forms. You can also view, edit, and delete the notes that you have saved.

To create Notes

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
5. In the **Edit Notes** window, under **Details**, in the **Title** box, type a title for the note you want to save.
   If a note already exists, click **Create New Notes**, and then under **Details**, in the **Title** box, type a title for the note you want to save.
6. Type any additional information in the **Information** box.
7. Click **Save**.
8. In the **Edit Notes** window, click **OK**.
9. In the **Settings** window, click **OK**.

To edit Notes

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
5. In the **Edit Notes** window, under **Title**, select the title of the note that you want to edit.

6 Click **Edit Notes**, and modify the information under **Details**.
You can change the category, modify the title, and edit the additional information that you have provided..
7 Click **Save**.
8 In the **Edit Notes** window, click **OK**.
9 In the **Settings** window, click **OK**.

To delete Notes

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Web** tab.
3 In the left pane, click **Identity Safe**.
4 Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
5 In the **Edit Notes** window, under **Title**, select the title of the note that you want to delete.
6 Click **Delete Notes**.
7 In the confirmation dialog box, click **OK**.
8 In the **Edit Notes** window, click **OK**.
9 In the **Settings** window, click **OK**.

About exporting and importing Identity Safe data

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer. The backup files are saved as .DAT files.

You can protect the files that you backed up with a password. Symantec recommends that you use a password to keep your Identity Safe data more secure. The backup password does not need to be the same as your Identity Safe password. You must provide the password when you restore the Identity Safe data that you backed up.

You can import your Identity Safe data from the file that you previously backed up. You can also import the Identity Safe data from the portable profile.

When you import the Identity Safe data you have the following options:

- Merge the imported data in to the vault that you are currently logged in .
- Replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

You can also delete the data once the import is complete.

Exporting your Identity Safe data

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer.

You can retrieve Identity Safe data when your product expires.

To export your Identity Safe data

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Backup Identity Safe Data** row, click **Configure**.
5. In the **Export Identity Safe Data** window, select the **Backup File Format**.
   You can select one of the following:
   - Identity Safe Backup Format
   - Plain text
6. In the **File Name** box, type, or browse to the location to which you want your data saved.
7. Type the name that you want to assign to the file with a .DAT suffix.

8 If you want to back up your data with a password for more security, type and confirm the password.

9 Click **OK**.

10 In the confirmation dialog box, click **OK**.

Importing your Identity Safe data

You can import your Identity Safe data from the file that you previously backed up. You can also import the Identity Safe data from the portable profile that you saved in the older version of Norton Internet Security.

You can merge the imported data in to the vault that you are currently logged in or replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

The **Merge with existing data** and **Replace existing data** options appear only when you import Identity Safe data from a backup file.

When you import Identity Safe data from local or portable profile, you can only merge the data. The **Delete Original data once merged** option appears when you import the data from local or portable profile. By default this option will be enabled.

To restore your data

1 In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Web** tab.

3 In the left pane, click **Identity Safe**.

4 Under **Identity Safe**, in the **Import Identity Safe Data** row, click **Configure**.

5 In the **Import Identity Safe Data** window, under **Import my data from**, select one of the following options:

- **Portable Profile (Drive: Drive:\)**

  This option appears only if you connect an external drive with a portable profile.
- **Local Profile**

  Select this option if you want to import the Identity Safe data from your local vault to online vault. This option appears only if you are logged in to your online vault.
- **Backup File**

  If you select this option, you must type or browse to the location of the file from which you want to import the data.

6 If you backed up your data with a password, in the **Password** box, type the password.

7 If you want to import the data from a backup file, under **While importing data**, select one of the following options:

- **Merge with existing data**
- **Replace existing data**

8 Click **OK**.

9 In the confirmation dialog box, click **OK**.

About Identity Safe Options

Identity Safe Options lets you configure the way you want Identity Safe to collect, store, and display the login information for the Web pages you visit. You can configure Identity Safe to display your cards that you created for the Web sites that have forms. You can also configure the autofill settings for the Web sites that contain security threats.

Symantec recommends you to keep the default settings for logins.

You can configure the following options in the **Identity Safe Options** window:

Offer to save my credentials when I log in to web sites	Prompts you to save the login credentials for the Web sites that you visit.
Display my Logins each time I visit a page with multiple Logins	Configures Identity Safe to display your logins each time you visit a Web site that has multiple logins.
Autofill my logins when I visit websites	Autofills your login details when you visit a Web site.
Display my Identity Cards each time I visit a page with fillable form	Displays your Identity Cards each time you visit a Web page with forms to fill your personal details.

In addition, you can use the **Autofill sites containing security threats** option to specify how you want Identity Safe to respond to the Web sites that have security threats.

About Identity Safe Password & Security options

You can use Identity Safe Password & Security to change your Identity Safe password. You can also use this option to set the level of security that you want for Identity Safe password usage.

The following sections let you change the Identity Safe password and set security levels for your password:

Identity Safe Password	Change your Identity Safe password and set a new password hint using the **Change Password** option.

Password Security	

	Specify the Identity Safe password security level. Identity Safe provides four levels of security to protect your Identity Safe password. Choose one of the following options: ▪ **Ask for my password at the beginning of each Login session** Prompts for your Identity Safe password the first time you access Identity Safe. As long as you are logged in to Windows, you do not need to provide the password again. You should use this option to make your login credentials more secure. ▪ **Ask for my password before filling out a Login** Prompts for your Identity Safe password with every online form before it autofills any login. You can specify that individual logins require the entry of your Identity Safe password before autofill occurs. ▪ **Automatically log out of Identity Safe if computer is inactive for** Automatically logs you out of Identity Safe when your computer is idle for the time that you specify. You can select 15, 30, or

	45 minutes. This option is useful if you are frequently in an area where other people have access to your computer. ■ **No password needed. Automatically log me in when Windows is started** Set this option if you want to automatically log in to Identity Safe when Windows is launched. Symantec recommends that you do not choose this option. The setting of this option is specific to Windows user account . You must validate your Identity Safe password each time you change the security level of the vault to a setting that is less secure than the current security level.

Changing the Identity Safe password

You should change your Identity Safe Password regularly to prevent unauthorized access to your personal information in Identity Safe.

If you want to change the Identity Safe password of your online vault, the password you provide must have the following charecteristics:

- At least eight characters
- At least one capital letter
- At least two numerals (0 through 9)
- At least one symbol (for example, * > & $ %)

- The password must not match with your Norton Account user name or password.

You can set your password hint here if you did not provide it when you configured Identity Safe.

To change the Identity Safe password

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Web** tab.
3. In the left pane, click **Identity Safe**.
4. Under **Identity Safe**, in the **Identity Safe Password & Security** row, click **Configure**.
5. In the **Password & Security** window, click **Change Password**.
6. In the **Change Identity Safe Password** window, type the current password and the new password, and confirm the new password.
7. Click **OK**.
8. In the confirmation dialog box, click **OK**.

About Norton Toolbar

When you install Norton Internet Security, it adds **Norton Toolbar** to Internet Explorer, Firefox, and Chrome Web browsers.

You have the following options in the **Norton Toolbar**:

Norton menu	Lets you access the Web Settings and other settings. The following options are available in the **Norton** menu: ▪ **Report Site** ▪ **Minimize Toolbar** ▪ **Settings** ▪ **Community Buzz** ▪ **Go to Norton Safe Web website** ▪ **Enable Norton Safe Web** ▪ **Enable Norton Safe Search/Disable Norton Safe Search** ▪ **My Norton Account** ▪ **Launch Tutorial** ▪ **Help** The **Minimize Toolbar** option appears only in the Internet Explorer browser. Also, the **Community Buzz** option is available only in English-language versions of Windows.

Norton Safe Search	Lets you perform an enhanced Internet search using Norton Safe Search. You can type a search string in the **Norton Safe Search** box and perform a search. When you search using the search box, a pop-up window appears and displays the relevant search results. Norton Internet Security uses the Ask.com to display the search results. By default, the **Norton Safe Search** box is hidden. After you install Norton Internet Security and connect to Internet, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search.
Safe Web indicator	Lets you know if the Web site you visit is safe or unsafe. The Antiphishing and Norton Safe Web options under the **Safe Surfing** section on the **Web** tab of the **Settings** window, analyze the security level of the Web sites you visit. It then displays the results in the **Norton Site Safety** pop-up window.

Identity Safe menu	Lets you view the logins and cards that you have saved in Identity Safe. Some Web sites have forms to fill or require login information. You can use the **Identity Safe** menu to fill the details in those Web sites. The **Identity Safe** menu displays the list of all logins and cards that you saved. You can select a login from the list and a use it to log in to the Web site. You can also select a card from the list and use to fill forms. You can access all the Identity Safe options and the **Settings** window from the **Identity Safe** menu. You should be logged in to any of the Identity Safe vault to access the **Identity Safe** menu.

Norton Internet Security lets you install the **Norton Toolbar** for free even after you uninstall the product. When you uninstall Norton Internet Security, it offers to leave the **Norton Toolbar** without any cost to search and browse safely over the Internet. However, when you choose to install the **Norton Toolbar**, the only features that you have are Norton Safe Search and Norton Safe Web.

Your computer must be connected to the Internet to avail this option. Norton Internet Security does not offer to leave the **Norton Toolbar** if you upgrade your product to the latest version or choose to reinstall another Norton product.

Hiding and showing the Norton Toolbar

You can hide the **Norton Toolbar** if you do not want to see the evaluation of every Web site that you visit. When you hide the toolbar, Norton Internet Security does not display the **Norton Site Safety** pop-up window. However, Norton Internet Security notifies you about suspicious and fraudulent Web sites or if an error needs your attention.

To hide or show the Norton Toolbar in the Internet Explorer and FireFox Web browsers

1. At the top of your browser window, click **View**.
2. On the **Toolbars** submenu, do one of the following:
   - Uncheck **Norton Toolbar** to hide the toolbar.
   - Check **Norton Toolbar** to show the toolbar.

Accessing Identity Safe settings from the Norton Toolbar

When you install Norton Internet Security, it adds the **Norton Toolbar** to the Internet Explorer, Firefox, and Chrome Web browsers. The **Identity Safe** menu on the **Norton Toolbar** provides quick links to access the options under Identity Safe.

To access the Identity Safe settings from the Norton menu

1. Start your Web browser.

2 On the **Norton Toolbar**, in the **Norton** menu, select one of the following:

Report Site	Lets you report to Symantec about the current Antiphishing evaluation.
Minimize Toolbar	Lets you minimize the Norton Toolbar. When you check this option, the **Identity Safe** phrase and the Safe Web phrase disappear and only the **Identity Safe** and Safe Web indicators remain. In addition, the size of the **Norton Safe Search** box is reduced. The **Minimize Toolbar** option appears only in the Internet Explorer browser.
Settings	Lets you open the **Web** tab in the Norton Internet Security **Settings** window.

Community Buzz	Lets you view the community site rating of the Web sites you visit. You can click **Community Buzz** to know further details about the Web sites. Norton Safe Web rates the sites and provides detailed reports. In addition, you can see user reviews and post your reviews about the Web sites. When you have not opened any Web site, you can click **Community Buzz** to visit the Norton Safe Web site. You can provide the address of any Web site and find the security details, Norton rating, and community reviews of the Web site. The **Community Buzz** option is available only in English-language versions of Windows.
Go to Norton Safe Web website	Lets you open the Norton Safe Web site http://www.safeweb.norton.com.
Enable Norton Safe Web	Lets you turn on the Norton Safe Web feature which provides a safe online browsing experience. The following are the unique features of Norton Safe Web: ▪ Displays the site safety rating icons next to the search results ▪ Displays the site safety rating icons when you are on a Web site

Enable Norton Safe Search/ Disable Norton Safe Search	Lets you view the **Norton Safe Search** box. You can type a search string in the Norton Safe Search box and perform a search. The search box displays relevant search suggestions in a pop-up window. By default, the **Norton Safe Search** box is hidden. After you install Norton Internet Security and open Internet Explorer or Firefox, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search. If you want to disable Norton Safe Search, you can use the **Disable Norton Safe Search** option.
My Norton Account	Lets you open the Web site https://www.mynortonaccount.com. Norton Account lets you register your product with Symantec and manage all of your Norton products in one place.
Launch Tutorial	Lets you view the online tutorial to learn more about Identity Safe.
Help	Lets you view the **Norton** menu help page.

Accessing the Identity Safe menu

The Identity Safe menu on the **Norton Toolbar** lets you view and manage the logins, Identity cards, and notes that you saved. You can also access the **Web** tab of the **Settings** window using the **Identity Safe** menu.

In addition, you can do the following:

- Navigate to any Web site for which you have saved the login credentials.
- Submit feedback about your experience with Identity Safe.
- Export your Identity Safe data.
- Import your Identity Safe data from the file you backed up or from the portable profile.
- Convert your local vault to online vault.

When you visit any login Web page without setting up your Identity Safe , a menu bar appears in the **Norton Toolbar**. You can use the **Setup** option that is available in the menu bar to set up Identity Safe.

Identity Safe menu lets you view the logins that you saved even after the product expires.

To access your logins from the Identity Safe menu

1 Start your Web browser.

2 On the **Norton Toolbar**, in the **Identity Safe** menu, select one of the following:

Merge Portable Data (Drive:\)	Lets you merge the Identity Safe data from your portable profile that you have created from the previous versions of Norton Internet Security. This option appears in the **Identity Safe** menu only if you have connected an external drive with portable profile.
Stop ignoring this page	You can select this option if you want to autofill the login information in the current Web page. This option appears in the **Identity Safe** menu only if you select **Ignore this page** option under **Options**.
Recently Used Logins	Lets you view the list of logins that you used recently in that computer. You can view only the latest five logins that you used.
All Logins	Lets you view the list of all the logins you have stored in Identity Safe.

Options

Lets you view the various options that are available in Identity Safe.

The options are:

- **Ignore this page**

  You can select this option if you do not want to autofill the login information in the current Web page.
- **Edit Logins**

  Lets you open the **Edit Logins** window.
- **Edit Identity Cards**

  Lets you open the **Edit Identity Cards** window.
- **Edit Notes**

  Lets you open the **Edit Notes** window.
- **Settings**

  Lets you open the **Web** tab in the **Settings** window.
- **Export**

  Lets you open the **Export Identity Safe Data** window.
- **Import**

  Lets you open the **Import Identity Safe Data** window.
- **Move to Online**

  Lets you open the **Move Identity Safe Data Online** window.

  You can move your Identity Safe data that you stored in your local vault to online vault. You

	must log in to your Norton Account to move your data online. This option appears in the **Identity Safe** menu only when you are logged in to your local vault.
Report Issue	Lets you open the Norton Feedback Web site. You can submit feedback on your experience with Identity Safe. You can also submit the problems that you encountered with Identity Safe. You can select from the list of problems or you can describe your problem.
Fill Login Fields	Lets you view the login information that you have saved for that Web site.
Fill with Identity Card	Lets you use a card while you are on a Web page that has forms. The option displays the cards that you saved from which you can choose the one you want to use to fill the form. The option appears only when you are on a Web site that has forms.

Log in to Identity Safe/Log out of Identity Safe	Lets you log out of or log in to Identity Safe. You should log out of Identity Safe to secure your Identity Safe data when you are away from your computer.

Monitoring protection features

7

This chapter includes the following topics:

- About Security History

About Security History

Security History window lets you do the following:

- View the summary of alerts and event messages.
- View the results of scans that are run on your computer.
- View the items that you submitted to Symantec Security Response Web site.
- Manage Quarantine items.
- Monitor the security tasks that your products perform in the background.

Security History lets you monitor the security tasks that your product performs in the background. In addition, the alerts that you receive can be reviewed at any time in Security History. If you cannot review an alert when you receive it, you can review it later in Security History.

The alerts, scan results, and other security items that are related to various product features appear under their respective categories in the **Security History** window. For example, the security items that are related to the Quarantine feature appear under the **Quarantine** category. In addition, the **Security History**

window displays details of each item in the **Details** pane.

Based on their functionalities, Security History broadly organizes all categories into the **All Activity**, **Protection and Performance**, **Submissions and Errors**, and **Informational** groups.

By default, the following information categories are available in the **Security History** window:

- **Recent History**
- **Full History**
- **Scan Results**
- **Resolved Security Risks**
- **Unresolved Security Risks**
- **Quarantine**
- **SONAR Activity**
- **Firewall – Network and Connections**
- **Firewall – Activities**
- **Intrusion Prevention**
- **Download Insight**
- **AntiSpam**
- **Identity**
- **Norton Product Tamper Protection**
- **Performance Alert**
- **Metered Network**
- **Sites reported to Symantec**
- **Norton Error Reporting**
- **Email Errors**
- **Norton Community Watch**
- **Silent Mode**
- **LiveUpdate**

You can view the security items based on the category of events that you select and the search string that you provide. Norton Internet Security restricts the number of search results that appear on each page in the

Security History window. Therefore, Security History divides the items that are returned for any search criteria and displays them on separate pages. You can use the pagination scroll at the bottom of the window to navigate to different pages sequentially. In case you want to view a specific page, you can use the **Go to page** option to open the page. The maximum number of items that appear per page is 100.

Based on the security status of an item in an information category, you can take an appropriate action to resolve a risk or a threat. The actions that you can perform include the following:

- Restore and exclude a quarantined item.
- Remove an item from Security History.
- Submit an item to Symantec for further analysis.
- Trust or restrict devices on a selected network.
- Remove the trusted or restricted status of devices on the selected network.
- Allow a selected program to access the Internet.
- Configure Norton Internet Security to notify you when it blocks a selected attack signature.

Norton Internet Security also lets you save the security events history. You can view the security event information whenever you want. If you want to analyze the security events for a particular day, you can save the Security History logs for that day. You can later import the file into Security History and analyze the data.

Opening Security History

Security History provides a record of all the activities that Norton Internet Security performed on your computer.

You can access Security History from the following areas:

- Norton Internet Security advanced window

- Various alert windows and notifications
- Notification area of the Windows taskbar
- **Threats Detected** section in different **Scan** windows

To open Security History

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **History**.

Viewing items in Security History

Security History provides a record of all the activities that Norton Internet Security performed on your computer.

You can view details about all the activities including:

- Security History alerts and event messages
- Results of different scans
- Information that you submitted to Symantec Security Response Web site
- Quarantined items
- Norton Internet Security firewall activities
- Security tasks that Norton Internet Security performed in the background

Based on their functionalities, all Security History categories appear under the following groups in the **Show** drop-down list:

- **All Activity**
- **Protection and Performance**
- **Submissions and Errors**
- **Informational**

The items that are related to the various product features appear under their respective categories in the **Security History** window. For example, the security items that are related to the Quarantine feature appear under **Quarantine** category in the **Security History** window. In addition, the **Security History** window displays details of each item in the **Details** pane.

To view items in Security History

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **History**.

3 In **Security History** window, in the **Show** drop-down list, select the category of items that you want to view. Your options are:

Recent History	The **Recent History** view in the **Security History** window displays the alerts that you received during the last seven days. It lists the history of certain recent security events.
Full History	The **Full History** view in the **Security History** window displays the complete Security History.
Scan Results	You can scan your computer to check if any virus, spyware, malware, or security risk has infected your computer. The **Scan Results** view in the **Security History** window displays the details about the scans that are run on your computer.

Resolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Resolved Security Risks** view in the **Security History** window displays a list of security risks that Norton Internet Security has detected and then repaired, quarantined, or removed. The quarantined items are listed in the **Quarantine** view. You can also view the quarantined items in the **Quarantine** view.
Unresolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Unresolved Security Risks** view in the **Security History** window displays a list of security risks that Norton Internet Security was not able to repair, remove, or quarantine. Security History does not let you clear logs for the unresolved security risks.

Quarantine	The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide an action to take on them. The **Quarantine** view in the **Security History** window displays all of the security risks that are isolated in the Security History Quarantine.
SONAR Activity	Symantec Online Network for Advanced Response (SONAR) identifies new threats based on the suspicious behavior of applications. SONAR detects and protects your computer against malicious code even before virus definitions are available through LiveUpdate. The **SONAR Activity** view in the **Security History** window displays details about the security risks that SONAR detects. This category also lists any activity that modifies the configuration or the settings of your computer. The **More Details** option for this category provides details about the resources that this activity affects.

Firewall - Network and Connections	The firewall monitors the communications between your computer and other computers on the Internet. The **Firewall - Network and Connections** category in the **Security History** window displays information about the networks that your computer connects to. It also displays the actions that you have taken to trust or to restrict networks and computers. This category also displays a history of all of the TCP/IP network connections that were made with your computer. Network connections are logged when the connection is closed. The **Advanced Details** view in this category lets you modify trust or restrict settings for computers and networks.

Firewall - Activities	The firewall monitors the communications between your computer and other computers on the Internet. The firewall maintains rules to control Internet access to and from your computer. The **Firewall - Activities** view in the **Security History** window displays the rules that firewall creates. The rules that you create also appear in this view. The **Security History - Advanced Details** window for this category shows the created Program rules. It also lets you allow a blocked program rule.
Intrusion Prevention	Intrusion Prevention scans all the network traffic that enters and exits your computer for known threats. The **Intrusion Prevention** view in the **Security History** window displays details about recent Intrusion Prevention activities. The **Advanced Details** view in this category lets you control whether or not to be notified when Intrusion Prevention detects an **Intrusion Prevention** signature.

Download Insight	Download Insight processes any executable file that you download for analysis of its reputation level. It then informs you about the processing results based on the Download Insight settings. The **Download Insight** view in the **Security History** window displays details of all events that Download Insight processes and notifies. This view also contains information about the actions that you take based on the reputation data of the events.
AntiSpam	Norton AntiSpam protects your computer from exposure to unsolicited email. The **AntiSpam** view in the **Security History** window displays details about the email messages that AntiSpam has processed.

Identity	The various features of Identity Safe help you manage your identities and provide additional security while you perform online transactions. The **Identity** view in the **Security History** window displays the Antiphishing definitions that Norton Internet Security downloads when you run LiveUpdate to obtain the latest virus definitions.
Norton Product Tamper Protection	Norton Product Tamper Protection lets you protect your Norton product from any attack or modification by unknown, suspicious, or malicious applications. The **Norton Product Tamper Protection** view in the **Security History** window displays details about unauthorized attempts to modify Symantec processes. The tasks that your Symantec product blocks also appear in the list.

Performance Alert	The performance alert feature lets you view, monitor, and analyze the impact of the system activities on your computer. The **Performance Alert** view in the **Security History** window provides details about the impact of the processes that run on your computer. The details include the process name, the resources used, the extent of resource utilization, and the overall impact of the process on your computer. In addition, logs related to performance alerts and the programs that you have excluded from performance alerts also appear in the list.
Metered Network	Metered Broadband Mode lets you set up policies and restrict the Internet usage of Norton Internet Security. You can define the amount of network bandwidth that Norton Internet Security can use. The Metered Network view in the Security History window provides details about the actions that you performed to restrict the Internet usage of Norton Internet Security.

Sites reported to Symantec	In some cases, you might have submitted evaluation of certain Web pages to Symantec. The **Sites Reported to Symantec** view in the **Security History** window displays all the Web sites that you reported to Symantec to verify authenticity.
Norton Error Reporting	Norton Internet Security may generate errors in some cases. For example, an error can occur when you run LiveUpdate or scan a folder. Engine errors, timeout errors, and program errors are some of the types of errors. The **Norton Error Reporting** view in the **Security History** window displays any error that Norton Internet Security has generated.

Email Errors	Email errors include any failure that occurs when Norton Internet Security tries to send, download, or scan an email message that you send or receive. The **Email Errors** view in the Security History displays details about any Email Error alerts that you receive when an Email error occurs. Details include the **Error ID** and the **Error message**. This view also displays information about subject, sender address, and the recipient address that are related to the email message in the alert.
Norton Community Watch	The Norton Community Watch feature lets you submit any suspicious security or suspicious application data to Symantec for analysis. Symantec assesses the data to determine the new threats. The **Norton Community Watch** view in the **Security History** window displays a list of files that you have submitted to Symantec for analysis. Files, at various stages of submission, also appear in the list.

Silent Mode	Silent Mode suppresses alerts and notifications and temporarily suspends most of the background activities. The **Silent Mode** view in the **Security History** window displays the summary of the Silent Mode sessions. The summary includes the following information: ▪ The type of Silent Mode such as Silent Mode or Quiet Mode ▪ The type of program that turns on Silent Mode such as disk burning or TV recording ▪ The name of User-Specified program that turns on Silent Mode ▪ Whether Silent Mode is turned on or turned off
LiveUpdate	LiveUpdate obtains the latest virus definition updates and the program updates to all the Symantec products that you installed on your computer. These updates protect your computer from newly discovered threats. The **LiveUpdate** view in the **Security History** window shows the details of the LiveUpdate activities on your computer. The details include the severity, the status, and the duration of the LiveUpdate sessions on your computer.

4 Click a row to view details for that item.
If you want to view additional information about an item, click the **More Details** option in the **Details** pane. You can view the advanced details about the item in the **Security History-Advanced Details** window and take actions as needed. For some categories, the **More Details** option opens the **File Insight** window that displays the details about the selected Security History event. You must use the **Options** link in the **Security History** window to select an action that Norton Internet Security must perform on any item in these categories. The **Options** link is also available in the **File Insight** window for certain items.

About the Security History - Advanced Details window

The **Security History - Advanced Details** window lets you view more information about the items that you select in the **Show** drop-down list in the **Security History** window. You can also perform any action that is available for the selected item from this window.

The following table lists the categories that provide the advanced details about the Security History items:

Alert Summary	Displays the following information about the item: ▪ **Severity** This category displays the risk level of the selected item. The various levels of security risks are **High**, **Medium**, **Low**, and **Info**. ▪ **Activity** This category displays the activity that has caused Security History to identify the item as a security threat. ▪ **Date & Time** This category displays the date and time of the activity. ▪ **Status** This category displays the status of the action that has been taken on the item. ▪ **Recommended Action** This category displays the actions that you should take to resolve the security threat.
Advanced Details	Displays the detailed information of the item You can view the details such as category, risk level, risk category, submission date of the risk, risk status, risk description, and recommended actions for the items.

Actions	

	Displays the actions that are available for the selected item The options in the **Actions** view vary depending on the options that are available in the **Show** drop-down list in the **Security History** window. The following are some of the **Actions** options: ▪ **Trust** This action allows access to or from the selected computer or all of the unclassified computers on the selected network. This option is available in the **Security History – Firewall - Network and Connections** view. ▪ **Restrict** This action blocks access to or from the selected computer or all of the unclassified computers on the selected network. This option is available in the **Security History – Firewall - Network and Connections** view. ▪ **Remove trust** Removes the trusted status from the selected computer or from all of the unclassified computers on the selected network. This option is available in the **Security History – Firewall - Network and Connections** view. ▪ **Remove restriction**

	This action removes the restricted status from the selected computer or from all of the unclassified computers on the selected network. This option is available in the **Security History – Firewall - Network and Connections** view. ▪ **Allow** This action allows the selected program to access the Internet. This option is available in the **Security History – Intrusion Prevention** view. ▪ **Stop Notifying Me** This action prevents Norton Internet Security from notifying you when it blocks the selected attack signature in the future. This option is available in the **Security History – Intrusion Prevention** view. ▪ **Notify Me** This action allows Norton Internet Security to notify you when it blocks the selected attack signature in the future. This option is available in the **Security History – Intrusion Prevention** view.

Risk Management	Displays the links that provide the information that is related to the selected item For some Security History items, this view lets you access the relevant settings pane of the Norton Internet Security window.

About the File Insight window

The **File Insight** window provides details about any File of Interest that is available on your computer. This option of file analysis is available for the files that you download, scan, or use to perform an activity.

You can access the **File Insight** window in different ways. For example, you can use the various notifications, alerts, scan and performance-related windows, and the shortcut menu of the various files that are present on your computer to open the window. Security History provides a centralized location where you can access the **File Insight** windows of the various events that are related to Security Risks, Download Insight, and Performance.

The File Insight window lets you view more details of events that belong to some of the following categories in the **Security History** window:

Resolved Security Risks	Lets you view the detailed information about the resolved security risks in an organized way. The **Resolved Security Risks** category includes the infected files that Norton Internet Security repairs, removes, or quarantines. This category mostly includes the medium-level or the high-level risks that are either quarantined or blocked. The **File Insight** window provides details about the risk level, the origin, and the activity report of the resolved security risks on your system.
Unresolved Security Risks	Lets you view the detailed information about the unresolved security risks in an organized way. The **Unresolved Security Risks** category includes the infected files for which Norton Internet Security was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of the unresolved security risks on your system.

Quarantine	Lets you view the detailed information about quarantined security risks in an organized way. The **Quarantine** category includes the infected files that are isolated from the rest of your computer while they await your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of quarantined security risks on your system.
Download Insight	Lets you view the reputation details of a file that you download. You can use these details to determine the safety level of the file and then decide the action that you want to perform.
Performance Alert	Lets you view the performance details of any File of Interest that is available on your computer. The information includes the general details, the origin and lineage information, the resource usage, and the actions that the file has performed on your system.

The **File Insight** window provides various details about the Security History item. These details are classified in different tabs in the **File Insight** window.

You can select a tab to view more details about it. The **File Insight** window provides details about a file in the following tabs:

Details	Displays the information such as the confidence level, community usage of a file, how long ago the file was released and how stable the file is. Stability ratings of a file may vary depending upon your operating system. You can view details such as the signature and the date on which the file was created. You can determine if a file is a startup file and the date on which the file was last used.
Origin	Provides the lineage details of a file. You can view the file name and the URL of the source from where the file was downloaded. The lineage details of a file are available only if you downloaded or created the file after you installed Norton Internet Security. If the historical details of a file are not available, Norton Internet Security disables this **Origin** section.

Activity	Provides the details about the actions performed by the file on your computer. It also provides information about the resource usage of a process and the effect of the process on the overall CPU utilization of your computer.

Based on the severity of the security risks and the risk type, Norton Internet Security might display one or more of the following options in the **File Insight** window:

Locate	Lets you locate the file on your computer. This option is available at the top of the window.
Copy to Clipboard	Lets you copy the data from the **File Insight** window to the clipboard. After you copy the content to the Clipboard, you can open a document, paste the data, and save the document.
Options	Lets you access the **Threat Detected** window and view more details and perform actions.
Learn More	Lets you access the online tutorial page to get more information about the file.

About the Threat Detected window

The **Threat Detected** window appears whenever Norton Internet Security detects a security risk on your computer. You can use this window to view details about the risk and select an action for the risk. Sometimes, you may want to access the **Threat Detected** window for the same risk again. In that case, the window can be opened at any time from Security History. Security History is the centralized location where you can access the **Threat Detected** windows of risks that belong to some of the following categories:

Resolved Security Risks	This category includes the security risks or the infected files that Norton Internet Security has detected and then repaired, quarantined, or removed.
Unresolved Security Risks	This category includes the security risks or the infected files that Norton Internet Security was not able to repair, remove, or quarantine.
Quarantine	This category includes the security risk items that are isolated from the rest of your computer while they await your attention for a suitable action.

The action options in the **Threat Detected** window for a risk vary depending on the risk type and its severity

level. The following are some of the options that are available in this window:

Restore & exclude this file	Returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans
Remove this file	Removes the security risk from your computer and quarantines it
Exclude this program	Excludes the security risk from future scan
Remove from history	Removes the selected security risk item from the Security History log
Get help	Takes you to the Symantec Security Response Web site
Submit to Symantec	Sends the security risk to Symantec

Searching in Security History

You can search the items that are listed in Security History. You can use the **Quick Search** option to find items using a keyword or the name of a security risk. If you want to view all of the Security History items that pertain to a particular security risk, you can filter the items using **Quick Search**. For example, if you want to view all of the alerts that Auto-Protect has generated, you can type Auto-Protect and filter the list.

You can clear the search results and return to the current Security History list by clicking the black cross (x) icon in the **Quick Search** box.

The **Quick Search** option works on the current view only. If you want your search to include all of the items in Security History, you must select the **Full History** view.

To search in Security History

1. In the **Security History** window, in the **Quick Search** text box, type the name of the item that you want to search.
2. Click **Go**.

Exporting or Importing Security History information

Norton Internet Security lets you export the Security History events to a file. You can export and save the Security History events and view them at your leisure.

For example, you can analyze the security events on a particular day. You can use the **Quick Search** option to obtain a list of all of the items that are related to a particular security risk. You can then use the **Export** option to save the list in the Security History log. You can later import the log file and analyze the data.

Security History stores the information in a separate file. When the file size reaches its maximum size limit, information that is related to new events overwrites the information that is related to older events. You can export the log periodically, if you want to keep the entire Security History information.

You can save your log file in one of the following file formats:

- Security History Log Files (.mcf)

  The .mcf file format is the Security History Log Files format and is proprietary to Symantec.

  When you use this file type option, you can view the file only in the **Security History** window.
- Text Files (.txt)

The data is saved in a comma-separated text format.

When you use this file type option, you can open and view the file externally without using Security History.

You can import only the log files that have .mcf file extension. When you import a log file, the exported list of Security History information in the log file appears. This list replaces the current security events list. You can select an option in the **Show** drop-down list to view the option-specific details that are saved in the log file. To revert to the current Security History list you must click the **Close file: *file_name*.mcf** link.

To export Security History information

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **History**.
3. In the **Security History** window, in the **Show** drop-down list, select an option.
4. Click **Export**.
5. In the **Save As** dialog box that appears, navigate to a location and specify the name for the file. The category name in the **Show** drop-down list appears as the default file name. You can provide a file name of your choice.
6. In the **Save as type** box, select the format in which you want to save your log file.
7. Click **Save**.

To import Security History information

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **History**.
3. In the **Security History** window, click **Import**.
4. In the **Open** dialog box that appears, browse to the folder that has the file you want to import.

5 Select the .mcf file and click **Open**.
You can only open log files of .mcf format in the **Security History** window. You can open and view log files of .txt file externally without using Security History.
In the import mode, you cannot make modifications to the information. For example, you cannot clear the logs. You can revert to the current Security History list by closing the file.

Managing items in the Quarantine

The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide on an action to take on them. Quarantined items are isolated from the rest of your computer so that they cannot spread or reinfect your computer. In some cases, you may have an item that you think is infected, but is not identified as a risk by the Norton Internet Security scans. You can manually place such items in the Quarantine.

You cannot open quarantined items accidentally and spread the virus, but you can evaluate the quarantined items for possible submission to Symantec.

The Security History Quarantine includes the following groups of items:

Security risks	Includes the items such as spyware and adware that are generally low risk and that another program requires to function properly. You can restore these items if necessary.
Security threats	Includes viruses and other high-risk items.

Once an item has been quarantined, you have several options. All of the actions that you take on quarantined items must be performed in the Security History Quarantine.

To open the Quarantine

1. In the Norton Internet Security main window, click **Advanced**.
2. In the **Computer Protection** pane, click **Quarantine**.

To perform an action on a quarantined item

1. In the **Security History** window, in the **Quarantine** view, select the item on which you want to perform the action.
2. In the **Details** pane, click **Actions**.
   You can use the **More Details** link to view more details about the item before you select an action for it. The link opens the **File Insight** window that contains more information about the risk.

3 In the **Threat Detected** window, select the action that you want to perform. Some of the options are:

Restore & exclude this file	Returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans This option is available for the detected viral and non-viral threats.
Remove from history	Removes the selected item from the Security History log
Submit to Symantec	Sends the selected item to Symantec for evaluation of the security risk In some cases, Norton Internet Security might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can use this option to submit the item to Symantec for further analysis.

You can also navigate to this window by using the **Options** link in the **File Insight** window for some risks.

4 Follow the on-screen instructions.

Adding an item to the Quarantine

Security History Quarantine provides a safe location on your computer in which you can isolate items while you decide on an action to take on each item.

The **Quarantine** view in the **Security History** window displays a list of quarantined items. You can view the name and the risk status of each quarantined item.

You can manually add an item to the Security History Quarantine. You can use the **Add to Quarantine** option in the **Quarantine** view in the **Security History** window to quarantine the items that you suspect are infected. This action has no effect on the items that are already quarantined.

You cannot add a known Good File to Quarantine.

To add an item to the Quarantine

1. In the **Security History** window, in the **Quarantine** view, click **Add to Quarantine**.
2. In the **Manual Quarantine** dialog box, in the **Description** text box, type a short name for the item that you want to add.
   This text appears in the Quarantine, so you should use a recognizable description.
3. Click **Browse**.
4. In the **Select File to Quarantine** dialog box, browse to the item that you want to add, select it, and then click **Open**.
5. Click **Add**.
6. Click **Close**.

Restoring an item from the Quarantine

Some programs rely on other programs that are classified as security risks to function. The program may not function if a particular security file is removed. All of the removed security risks are automatically backed up in the Security History Quarantine. This way, Norton Internet Security lets you restore any risk to regain the functionality of a program that requires the risk program to run.

For example, a shareware or freeware program that you download may use adware to keep its price low. In this case, you can allow the security risk program to

remain on your computer or restore it if Spyware Protection has removed it.

Some quarantined items are successfully disinfected after Norton Internet Security rescans them. You can also restore such items.

If you restore an item to a directory other than its original location, it may not function properly. Therefore, it is recommended that you reinstall the program.

To restore an item from the Quarantine

1. In the **Security History** window, in the **Quarantine** view, select the item that you want to restore.
2. In the **Details** pane, click **Actions**.
3. In the **Threat Detected** window, click **Restore & exclude this file**.
   This option returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans.
4. In the **Quarantine Restore** window, click **Yes**.
   In case of non-viral threats, you can use the option that is available in this window to exclude the security risk. Norton Internet Security does not detect the security risks that you exclude in the future scans.
5. In the **Browse for Folder** dialog, select the folder or drive where you want to restore the file and then click **OK**.
6. Click **Close**.

Manually submitting an item to Symantec

When a virus or other risk is detected, it is automatically submitted to Symantec Security Response Web site for analysis. If you have turned off the option to submit risks automatically, you can manually submit them from the Security History Quarantine. You must have an Internet connection to submit an item.

When you submit files to Symantec automatically or manually, you contribute to the effectiveness of your Symantec product. For example, you can submit an item that has not been detected during scanning that you believe may be a security risk. Symantec Security Response analyzes the file. If it is identified as a security risk, it is added to a future definition update.

Personally identifiable information is never included in submissions.

In some cases it is necessary for Symantec Security Response to block submissions of a particular type or volume. These items appear as **Not Submitted** in Security History.

To manually submit an item to Symantec

1. In the **Security History** window, in the **Quarantine** view, select the item that you want to submit to Symantec.
2. In the **Details** pane, click **Actions**.
3. In the **Threat Detected** window, click **Submit to Symantec**.
4. In the dialog box that appears, click **OK**.

Customizing protection features

8

This chapter includes the following topics:

- Feature summary
- About turning off automatic features
- About customizing settings and options

Feature summary

Use the information in this section to familiarize yourself with the product.

This section includes the following information:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

For more information, select one of the sub-entries for this Help topic.

About virus and security risk protection features

Virus and security risk protection features provide comprehensive virus prevention and security risk detection for your computer. Known viruses are automatically detected and repaired. Instant messenger attachments, email message attachments, Internet

downloads, and other files are scanned for viruses and other potential risks. In addition, the definition updates that Automatic LiveUpdate downloads when your computer is connected to the Internet keeps you prepared for the latest security risks.

Your computer is continually monitored and protected from known and unknown threats by the following features:

Auto-Protect	Checks for viruses and other security risks every time that you run programs on your computer. Auto-Protect options let you customize the protection of your computer. Auto-Protect options are: ▪ Loads into memory when Windows starts, providing constant protection while you work. ▪ Checks for viruses and security risks every time that you use software programs on your computer. It also checks every time when you insert removable media, access the Internet, or use document files. ▪ Monitors your computer for any unusual symptoms that may indicate an active threat.
Automatic LiveUpdate	Notifies you of program updates and downloads definition updates automatically. See "About LiveUpdate" on page 49.

Compressed File Scan	Detects viruses, spyware, and other security risks in compressed files during manual scans. See "What to do if a security risk is found" on page 179.
Email Protection	Protects your computer against the threats that you may receive through email attachments. You can use the **Email Antivirus Scan** option and the **AntiSpam** option to configure your email program for protection against viruses and other security threats.
Insight Protection	Lets Norton Internet Security perform an Insight Network scan on your computer The Insight Network scan uses the virus definitions that are available locally and hosted in the Cloud. Norton Internet Security provides additional protection by using the most recent definitions from the Cloud, apart from the definitions that are available locally on your computer. See "About Insight Network scan" on page 134.

Instant Messenger Scan	Scans for and detects viruses in instant messenger attachments. Scans the instant messenger attachments for the supported instant messenger programs that were on your computer when you installed your product. New instant messenger programs must be configured in **Instant Messenger Scan** window.
Heuristic Protection	Detects the new and the unknown viruses by analyzing an executable file's structure, and behavior. Also, by analyzing other attributes such as programming the logic, computer instructions, and any data that is contained in the file.
Settings Password Protection	Protects Norton Internet Security Settings from unauthorized changes.
Quick Scan	Checks for the infections that have processes running in memory and the infections that the startup folders and files refer. Automatically runs once LiveUpdate updates your computer with program updates and definition updates. See "Running a Quick Scan" on page 119.

About spyware and other security risk protection features

Spyware and other security risk protection features provide protection against the latest security risks, such as spyware and adware. These features scan for existing risks and blocks new risks before they can be installed on your computer.

Spyware and other security risk protection features include the following:

Auto-Protect Spyware Blocking	Auto-Protect blocks the programs that have been identified as spyware or adware before they can be installed on your computer.
Security risk scan	By default, manual and scheduled scans search for spyware, adware, and other security risks. Auto-Protect scans for these items as well.
Security risk restore	If a scan removes a security risk program that another program relies on for functionality, you can restore the security risk program from Security History.

Security risk assessment	If you are unsure how to handle a program that is classified as a security risk, you can view the security risk assessment. The security risk assessment describes the level of impact that a security risk program has on your computer. You can access the security risk assessment from the **Risk Details** window. This window is available when the scan results require input before it process a security risk program.

About security protection features

Norton Internet Security includes a suite of security tools that help keep your computer safe from security risks.

Security protection features include:

Smart Firewall	Protects your computer from Internet attacks, port scans, and other suspicious behavior. See "About the Smart Firewall" on page 193.
Intrusion Prevention	Scans each piece of information that enters and exits your computer and automatically blocks any Internet attacks. See "About Intrusion Prevention" on page 244.

Trust Control	Detects when your computer connects to a new network. You can then allow or block connections from all computers that are connected to that network. See "About Smart Firewall Trust Control settings" on page 219.

About spam filtering features

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

Norton Internet Security provides several powerful features to reduce your exposure to unwanted online content.

Integration with email programs	Adds several options to the toolbar in supported email programs. See "About your email program toolbar" on page 265.

Allowed and Blocked Lists	■ Uses a user-defined address list to expedite the scanning of email. ■ Accepts all email messages from senders in the Allowed List. ■ Treats all email messages from senders in the Blocked List as spam. ■ Allows and blocks email messages from entire domains as well as individual email addresses. See "About Norton AntiSpam settings" on page 257.
Automatic import of addresses	Automatically imports lists of addresses from supported email programs to keep your list of allowed email senders and blocked email senders in sync. See "Identifying authorized senders" on page 261.
Web Query	Lets you query the Symantec Web servers to filter the spam email messages which the local filters fail to classify as spam. See "About Web Query" on page 267.
Automated update of spam definitions	Updates the copies of Symantec spam definition files automatically. See "Checking for updates manually" on page 55.

About Parental Control

The **Parental Controls** option lets you create your Norton Online Family account. Norton Online Family is a parental control application that provides a smart way to keep your children safe when they are online.

Norton Online Family helps parents to get a better understanding of what children do online, so that they can better protect and guide them.

You can use the **Online Family** icon at the bottom of the main window to create your Norton Online Family account. The icon may not be available with some versions of Norton Internet Security. In such case, you may not be able to access Norton Online Family options. You need to install Norton Safety Minder on each computer that your children use. If your children use the same computer, you need to create user accounts for each child and install Norton Safety Minder on the computer.

You can also use the **Parental Controls** link in the **Web Protection** pane in the Norton Internet Security advanced window to create your Norton Online Family account. Symantec recommends that you use your Norton Account credentials to register with Norton Online Family.

After you set up your account, you can configure your settings in Norton Online Family Web site to monitor your children's Internet activities. You can sign in to your Norton Online Family account at any time to view their online activities. You can also use the **Online Family** icon at the bottom of the main window to sign in to your account and view your child's Internet activities.

By using Norton Online Family, you can manage the Internet activities of your children in the following ways:

- Monitor and manage the Web sites that your children visit.
- Manage and monitor the computer usage of your children.
- Monitor and manage the social networking activities of your children.
- Monitor and manage the instant messaging activities of your children.

- Monitor and manage the Internet search that your children perform.
- Define House Rules for your children based on their age and maturity.

Norton Online Family may not be available with some versions of Norton Internet Security. In such case, you may not be able to access the Norton Online Family options.

About turning off automatic features

Your Symantec product is set by default to provide complete protection for your computer. Many of these settings include the automatic features that provide continuous protection. Under certain circumstances, you might need to turn off an automatic feature to complete a task.

When you have completed the task for which you turned off the automatic feature, make sure that you turn the feature on again.

See "Turning off Auto-Protect temporarily and turning it on again" on page 416.
See "Turning off or turning on spam filtering" on page 417.

Turning off Auto-Protect temporarily and turning it on again

If you have not changed the default option settings, Auto-Protect loads when you start your computer. Auto-Protect also guards against viruses, Trojan horses, worms, and other malicious threats. It checks programs for viruses when programs run and monitors your computer. It also checks the removable media for any activity that might indicate the presence of a virus. When Auto-Protect detects a virus or virus-like activity, it alerts you.

In some cases, Auto-Protect might warn you about a virus-like activity that you know are not the work of a virus. If you perform such an activity and want to avoid the warning, you can turn off Auto-Protect.

If you have set a password for settings, Norton Internet Security asks you for the password before you can view or change the settings.

When you turn off **Auto-Protect**, **SONAR Protection** and **Download Intelligence** are also turned off.

To turn off Auto-Protect temporarily

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Real Time Protection**.
3. In the **Auto-Protect** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.
5. In the dialog box that appears, in the **Select the duration** drop-down list, select how long you want to turn off Auto-Protect, and then click **OK**.

To turn on Auto-Protect temporarily

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, in the left pane, click **Real Time Protection**.
3. In the **Auto-Protect** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.

Turning off or turning on spam filtering

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

To control these spam mails you can use the spam filtering. By default, spam protection remains active. If for any reason you want to disable it, you can turn it off from within the program itself.

Turning off Norton AntiSpam increases your exposure to receive unsolicited email messages.

To turn off spam filtering

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. In the **AntiSpam** row, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off spam filtering.
7. Click **OK**.
8. In the **Settings** window, click **OK**.

To turn on spam filtering

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **Network** tab.
3. In the left pane, click **Message Protection**.
4. In the **AntiSpam** row, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.

Turning off or turning on Norton Community Watch

You can use the **Norton Community Watch** option to send information about a suspicious file to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. The Norton features such as Norton Insight and Insight Network use the Symantec assessed information to detect the security threats.

Norton Community Watch collects and submits detailed data about the Norton-specific errors and components only. It does not collect or store any personal information of any user.

You can use Security History to review the information that has been sent to Symantec.

To turn off or turn on Norton Community Watch

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Other Settings**.
4. In the **Norton Community Watch** row, do one of the following:
   - To turn off Norton Community Watch, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Norton Community Watch, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **OK**.

Turning off or turning on security protection features

There may be times when you want to turn off a security protection feature. For example, you might want to see if the Smart Firewall prevents a Web page from appearing as expected.

Turning off security protection features reduces your computer's security. When you turn off a feature, you can specify the amount of time it should remain off. After that time limit, the feature turns on automatically.

To ensure that your computer remains protected, you can turn on security protection features manually before the specified time frame concludes.

To turn off a security protection feature

1. In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 In the **Intrusion Prevention** row, move the **On/Off** switch to the right to the **Off** position.
5 In the **Smart Firewall** row, move the **On/Off** switch to the right to the **Off** position.
You may need to scroll the window to see the option.
6 In the **Settings** window, click **Apply**.
7 In the **Select the duration** drop-down list, select the amount of time that the security protection feature should be turned off, and then click **OK**.

To ensure that your computer remains protected, you can turn on security protection features manually before the specified time frame concludes.

To turn on a security protection feature

1 In the Norton Internet Security main window, click **Settings**.
2 In the **Settings** window, click the **Network** tab.
3 In the left pane, click **Smart Firewall**.
4 In the **Intrusion Prevention** row, move the **On/Off** switch to the left to the **On** position.
5 In the **Smart Firewall** row, move the **On/Off** switch to the left to the **On** position.
6 In the **Settings** window, click **Apply**.

Turning off or turning on Web settings

Web settings features are automatically turned on when you install Norton Internet Security. Web settings guards you against unsafe sites while you browse the Internet.

When you turn off and then turn on Web settings, you must log in to Identity Safe to use the various options of Identity Safe.

To turn off Web settings

1 In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Web** tab, and do the following:

- In the **Browser Protection** section, in the **Browser Protection** row, move the **On/Off** switch to the right to the **Off** position.
- In the **Download Intelligence** section, in the **Download Intelligence** section, in the **Download Intelligence** row, move the On/Off switch to the right to the **Off** position.
- In the **Identity Safe** section, in the **Identity Safe** row, move the **On/Off** switch to the right to the **Off** position.
- In the **Safe Surfing** section, in the **Antiphishing** row, move the **On/Off** switch to the right to the **Off** position.
- In the **Safe Surfing** section, in the **Norton Safe Web** row, move the **On/Off** switch to the right to the **Off** position.

3 Click **Apply**.

To turn on Web settings

1 In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, click the **Web** tab, and do the following:
   - In the **Browser Protection** section, in the **Browser Protection** row, move the **On/Off** switch to the left to the **On** position.
   - In the **Download Intelligence** section, in the **Download Intelligence** row, move the **On/Off** switch to the left to the **On** position.
   - In the **Identity Safe** section, in the **Identity Safe** row, move the **On/Off** switch to the left to the **On** position.
   - In the **Safe Surfing** section, in the **Antiphishing** row, move the **On/Off** switch to the left to the **On** position.
   - In the **Safe Surfing** section, in the **Norton Safe Web** row, move the **On/Off** switch to the left to the **On** position.
3 Click **Apply**.

About customizing settings and options

The default settings provide complete protection for your computer. However, you may want to adjust the settings to optimize system performance or disable the options that do not apply. You can change the product's settings to fit your work environment.

From non-admin accounts of your computer, you need administrator authentication to change product settings. If you are an administrator, keep in mind that the changes that you make apply to everyone who uses the computer.

However, you can configure your Identity Safe settings from any non-admin user account also. Each user account can individually configure and access their Identity Safe options only.

For more information, select one of the sub-entries for this Help topic.

Configuring Norton Internet Security settings

The default Norton Internet Security settings provide a safe, automatic, and efficient way to protect your computer. If you want to change or customize your protection, you can access most features from the main window.

If you want to control additional settings, such as Trust Control or Program Control, you can use the Norton Internet Security **Settings** window.

To configure Norton Internet Security settings for individual features

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click any of the settings tab to open it.
3. Move the switch to the desired position.
4. Click **Configure** for the feature that you want to change.
5. In the window that appears, make the necessary changes, and then click **OK**.
6. To apply the default settings in a specific section, click **Use Section Defaults** on the tab.
7. In the **Settings** window, do one of the following:
   - To save your changes and close the **Settings** window, click **OK**.
   - To save your changes without closing the **Settings** window, click **Apply**.
   - To apply the default settings, click **Default All**, and then click **OK** or **Apply**.
8. If **Security Request** dialog box appears, select the duration for how long you want to turn off a feature, and then click **OK**.

To configure Norton Internet Security Settings

1. In the Norton Internet Security main window, click **Settings**.

2 In the **Settings** window, configure your settings in the following tabs:

Computer	Lets you configure how you want Norton Internet Security to scan your computer for viruses and other security threats. You can also configure Norton Internet Security to obtain regular updates for complete protection of your computer. You can include additional protection to your computer by using the most recent definitions from Cloud during scans. Your options are: ▪ **AntiVirus and SONAR Exclusions** ▪ **Computer Scan** ▪ **Real Time Protection** ▪ **Updates**

Network	Lets you configure how you want Norton Internet Security to monitor your network activities. You can protect your computer against the threats that you might receive through email attachments, instant messaging program attachments. You can also configure the communication port that Norton products use to communicate with each other. In addition, you can protect your computer against intrusion attempts and unauthorized traffic. You can also configure Norton AntiSpam options to filter out unsolicited email messages. Your options are: **Intrusion Prevention** **Message Protection** **Network Security Settings** **Smart Firewall**

Web	Lets you safeguard your sensitive information and online transactions. You can manage your login information, such as email login credentials and your financial information, such as credit card details. You can also manage other personal information, such as social security number or driver's license number. You can also safely browse the Internet. In addition, you can protect your Web browser against attacks by malicious Web sites. You can also configure Norton Internet Security to indicate whether the executable file that you download is safe to install or not. Your options are: ▪ **Browser Protection** ▪ **Download Intelligence** ▪ **Identity Safe** ▪ **Safe Surfing**

General	Lets you configure the appearance and security of your product. In addition, you can configure how Norton Internet Security submits risk details to Symantec. You can specify your proxy settings to obtain definition updates. You can also configure Silent Mode, Performance Monitoring options, Idle Time Out duration, Monthly Report options, and other miscellaneous options. Your options are: ▪ **Norton Tasks** ▪ **Other Settings** ▪ **Performance Monitoring** ▪ **Product Security** ▪ **Silent Mode Settings**

If you set a password to access the **Settings** window, you must enter the password to view or configure settings even if you are an administrator. Therefore, ensure that you set an easy password. However, if you forget your settings password, you can reset the password in the window that appears when you choose to uninstall Norton Internet Security. You need not uninstall the product to reset your password. You can use the reset settings password option in the uninstall preference window to reset your password.

About Computer settings

The various options in the **Computer** tab let you configure how you want Norton Internet Security to scan your computer for viruses and other security threats.

Your options are:

AntiVirus and SONAR Exclusions	**AntiVirus and SONAR Exclusions** options let you specify the items that Norton Internet Security excludes from its scans. Scans and signatures are some items that you can exclude from scanning. **AntiVirus and SONAR Exclusions** options also let you choose which categories of risks you want Norton Internet Security to detect. AntiVirus and SONAR Exclusions reduce your level of protection and should be used only if you have a specific need.

Computer Scan	Norton Internet Security lets you run different types of scans to detect and prevent any virus infection on your computer. You can use the various **Computer Scan** options to select the scan type, file types to scan, and the scan schedule. You can also specify scanning of compressed files and Microsoft Office documents. You can perform a Full System Scan. You can also individually scan drives, folders, or files. The **Computer Scan** options also let you specify scans to detect rootkits, other stealth items, network drives, tracking cookies, and unknown security threats. The **Scan Performance Profiles** option lets you configure a Norton Internet Security scan based on the digital signature and trust level of the files on your computer. You must configure the Scan Performance Profiles settings before you run a scan or before a scan is scheduled to run. Norton Internet Security scans your computer according to the configuration that you specified in the Scan Performance Profiles settings.

Real Time Protection	

Real Time Protection option protects your computer by continuously checking for viruses and other security risks.

You can use the **Real Time Protection** options to control the scanning and monitoring of your computer.

Your options are:

- **Antispyware**

  Antispyware protects your computer against the security risks that can compromise your personal information and privacy. **Antispyware** options let you choose which categories of risk you want Norton Internet Security to detect for manual, email, and instant messenger scanning.
- **Auto-Protect**

  Auto-Protect loads into memory when Windows starts, providing constant protection while you work. Auto-Protect checks for security risks every time that you use software programs on your computer, insert removable media, access the Internet, or use document files. It also monitors your computer for any unusual symptoms that may indicate an active threat.

  You can use the **Auto-Protect** options to customize the protection of your computer.

	▪ **SONAR Protection** Symantec Online Network for Advanced Response (SONAR) provides you with real-time protection against threats by proactively detecting unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. SONAR Protection is quicker than the traditional signature-based threat detection techniques. SONAR detects and protects you against malicious code even before virus definitions are available through LiveUpdate. You can turn on this option to proactively detect unknown security risks on your computer. SONAR provides you the greatest control when low certainty threats are detected. ▪ **Enable Boot Time Protection** **Enable Boot Time Protection** starts Auto-Protect when you start your computer. It provides enhanced security level from the time your start your computer.

Updates	

Norton Internet Security protects your computer from vulnerabilities through the latest program and definition updates. Definition updates contain the information that lets Norton Internet Security recognize and alert you to the presence of a specific virus or security threat.

You can use the options in the **Updates** section to obtain the latest virus definitions and keep your computer secure from the latest security threats.

Your options are:

- **Automatic LiveUpdate**

  Automatic LiveUpdate automatically checks for definition updates and program updates to your virus protection when you are connected to the Internet.
- **Pulse Updates**

  In addition to the definition updates that Automatic LiveUpdate downloads, Norton Internet Security uses streaming technology to download the latest virus definitions. These downloads are called Pulse Updates. The Pulse Updates are lighter and faster, and keep your computer secure from the ongoing threats on the World Wide Web.
- **Automatic Download of New Version**

  Automatically downloads the

	latest available version and prompts you for free installation. To get the latest version, this option must be turned on. **Smart Definitions** Activates the Core Set virus definitions which contain the most important virus definitions that are required for latest security threats as viewed by Symantec. Turning on the **Smart Definitions** option minimizes download time, installation time, and system start time. Therefore, the Core Set results in faster performance of your computer.

About Network settings

The options in the **Network** tab let you configure Norton Internet Security to monitor your Internet activities.

You can configure Norton Internet Security to protect your computer against any threat that you may receive through email attachments or instant messenger attachments. You can also use the options in the **Network** tab to protect your computer against intrusion attempts and unauthorized traffic.

Your options are:

Intrusion Prevention	

	Intrusion Prevention scans all the network traffic to and from your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known vulnerability in the operating system or in a program. If the information matches an attack signature, Intrusion Prevention blocks the traffic from the suspicious computer. The following are some activities that you can do using the Intrusion Prevention options: ▪ View the list of Intrusion Prevention signatures. ▪ Exclude individual signatures from being monitored. ▪ Specify whether or not you must be notified when Intrusion Prevention signatures are detected. ▪ Activate AutoBlock for a specified duration to block all incoming traffic from a computer that continues to attack your system. ▪ View, restrict, or unblock the list of computers that AutoBlock blocks. ▪ View or unblock the list of computers that AutoBlock blocks. ▪ Determine whether or not you are notified when Intrusion Prevention activities are detected.

Message Protection	

	Message Protection protects your computer against the threats that you may receive through email attachments. You can use the **Email Antivirus Scan** option, the **AntiSpam** option, and the **Protected Ports Settings** option to configure your email program for protection against viruses and other security threats. Email Antivirus Scan protects you from the threats that are sent or received in email attachments. You can use the **Email Antivirus Scan** options to define how Norton Internet Security should behave when it scans email messages. Based on the options you choose, Norton Internet Security automatically scans the email messages that you send or receive. Norton AntiSpam lets you categorize the email messages that you receive into spam email and legitimate email. You can use the following **AntiSpam** options to do the following: ▪ Specify the addresses in your address book that Norton Internet Security must not add to the Allowed List. ▪ Specify the addresses or domains from which you want to receive or block email. ▪ Select the email programs in

	your computer with which you want to integrate Norton AntiSpam. ▪ Send feedback about any misclassified email message to Symantec for analysis. ▪ Classify the spam email messages effectively. **Instant Messenger Scan** option lets you customize the scanning of the files the instant messenger programs receive. You can select the supported instant messenger programs from which you may receive files. Norton Internet Security scans the files that you receive from the selected instant messenger programs. You can use the **Protected Ports Settings** option to protect the POP3 and SMTP ports that are associated with your email program. Norton Internet Security automatically protects the default SMTP port 25 and the default POP3 port 110. If your email program is not configured with the default ports, you can manually configure Norton Internet Security to protect your POP3 and SMTP ports.

Network Security Settings	

	The **Metered Broadband Mode** option lets you set up policies and restrict the Internet usage of Norton Internet Security. You can define the amount of network bandwidth that Norton Internet Security can use. The **Network Security Map** option provides a pictorial representation of the devices on the network to which your computer is connected. You can view the security status and trust level of the devices that are connected to the network to which your computer is connected. Network Security Map also lets you configure the communication port that Norton products use to communicate with each other. The **Welcome Screen** option displays the **Network Security Overview** window when you open Network Security Map. The **Proxy Server** option lets you specify the automatic configuration URL, proxy settings, and the authentication details for firewall or proxy server. In case of proxy servers, Norton Internet Security uses the Network Proxy Settings to connect to the Symantec server and the Internet. The following are also some activities that you can do using the Norton Security Map feature: ▪ View or modify details

	related to the computers or devices that are on your network. ▪ Grant or deny permissions to the networked devices to access your computer. ▪ Add or Remove any device in the Network Security Map. ▪ Change the trust control level for a particular Network address or an IP address.

Smart Firewall	Smart Firewall monitors communications between your computer and the other computers on the Internet. It also protects your computer from common security problems. You can use the Smart Firewall options to customize how the firewall monitors and responds to inbound communications and outbound communications. Your options are: ▪ **Advanced Settings** Lets you activate advanced protection features of Smart Firewall ▪ **Program Control** Lets you control settings for the programs that access the Internet ▪ **Trust Control** Lets you view the networks to which your computer is connected ▪ **Block All Network Traffic** Lets you configure how Norton Internet Security should control the network communications to and from your computer

About Web settings

Norton Internet Security provides complete protection for your sensitive information while you use the information on the World Wide Web.

The options in the **Web** tab let you configure Norton Internet Security to monitor your Internet activities.

Your options are:

Browser Protection	The Browser Protection feature checks for browser vulnerabilities in following browsers: ▪ Internet Explorer 6 or later ▪ Firefox 3.0 or later You must turn on the **Browser Protection** option to enable this feature.
Download Intelligence	Download Insight provides the **Download Intelligence** option to protect your computer against any unsafe file that you download using a Web browser. This feature supports only downloads using the HTTP protocol, Internet Explorer versions 6 or later, and Firefox 3.0 browser or later.
Identity Safe	The Identity Safe feature in Norton Internet Security lets you save and protect your logins. Identity Safe provides you the following features: ▪ **Export Identity Safe data** ▪ **Move Identity Safe Online** ▪ **Delete Identity Safe** ▪ **Identity Safe Options** ▪ **Identity Safe Password & Security** ▪ **Edit Identity Cards** ▪ **Edit Logins** ▪ **Edit Notes** ▪ **Import Identity Safe data**

Safe Surfing	Norton Internet Security protects your Internet Explorer, Firefox, and Chrome Web browsers with the **Safe Surfing** options. When the options under **Safe Surfing** are turned on, Antiphishing and Norton Safe Web analyze the security level of the Web sites that you visit. It then displays the security information in the **Norton Site Safety** pop-up window.

About General settings

You can use General settings to schedule your product tasks and configure different Norton Internet Security settings. You can access the General settings options under the **General** tab in the **Settings** window. You can also configure the security settings of your product from General settings.

By using General settings, you can do the following:

- Schedule your Norton Tasks.
- Configure the General settings of your product.
- Monitor the performance of your system.
- Configure the security settings.
- Customize the Silent Mode settings.

Your options are:

Norton Tasks	

	Lets you configure your Norton Tasks settings. Your options are: ▪ **Automatic Resume Delay** This option delays the automatic background tasks for a specific duration even if your computer is idle for that period. You can specify Automatic Resume Delay duration for a period of one minute to 20 minutes. By default, the **Automatic Resume Delay** option is set to 10 minutes. ▪ **Automatic Tasks Delay** Lets you delay the start-up of Norton-specific programs on your computer that run automatically when you turn on your computer. Automatic Tasks Delay does not delay Norton Internet Security protection. You can specify Automatic Tasks Delay duration for a period of one minute to 20 minutes. The default duration is 20 minutes. ▪ **Idle Time Optimizer** Lets you configure Norton Internet Security to defragment your boot volume or the local disk that contains the boot

	volume when your computer is idle. When the option is turned on, Norton Internet Security automatically schedules the optimization after you install an application on your computer. Optimization improves the performance of your computer by defragmenting the fragmented parts of the disk. **Idle Time Out** Lets you specify the Idle Time Out duration after Norton Internet Security identifies your computer as idle. You can specify the Idle Time Out for a period of one minute to 30 minutes. The default duration is 10 minutes. **Norton Task Notification** Lets you configure Norton Internet Security to show or hide the notifications that appear when automatic Norton Tasks are started.

Other Settings	

	Lets you configure the miscellaneous settings. Your options are: **Power Saving Mode** Lets you save your battery power by suspending the Norton Tasks when your computer is on battery power. By default, this option is turned on. **Monthly Report** Lets you view the Monthly Report for the last 30 days. You can configure the Monthly Report options to remind you to view Monthly Report. **Special Offer Notification** Lets you configure Norton Internet Security to notify you about special offers on the latest Norton products, add-ons, and other useful information from Symantec. **Insight Protection** Lets Norton Internet Security to perform an Insight Network scan on your computer. The Insight Network scan uses the virus definitions that are available locally and hosted in the cloud. Norton Internet Security provides additional protection by using the

	most recent definitions. ▪ **Norton Community Watch** Lets you submit selected security and application data to Symantec for analysis. Symantec analyses the data to determine any possible security risks and provides you the useful statistical information about the applications. The **Detailed Error Data Collection** option lets you allow or deny some of the detailed data submissions. These detailed data may vary depending on the Norton-specific errors and components. You can use the **Always**, **Never**, and **Ask Me** options to configure the submissions.

	Parental Controls have not been installed Lets you install Norton Online Family. Norton Online Family is a parental control application that helps you protect your child from Internet dangers and online predators. It lets you grant permission for your child to access Web sites based on the age and maturity of your child. You can use the **Click here to install** link to install Norton Safety Minder and to configure Norton Online Family. Norton Safety Minder is an application that needs to be installed on each computer that your child uses. After you install Norton Online Family, the **Parental Controls have not been installed** option changes to **Norton Online Family is installed**. The **Click here to install** link also changes to **Click here to configure**. You can use the **Click here to configure** link to log on to Norton Online Family and modify the Norton Online Family settings.

Performance Monitoring	

	Lets you monitor the performance of your computer. **Performance Monitoring** When you turn on the **Performance Monitoring** option, Norton Internet Security monitors the CPU usage and memory usage of your computer. You can also monitor the important system activities that you performed for the last three months in the **Performance** window. In addition, Norton Internet Security notifies you with performance alerts when there is high usage of your system resources by a program or process. Your options are: **Performance Alerting** Lets you configure Norton Internet Security to detect and notify you about the increased usage of your computer resources by any program or process. Norton Internet Security notifies you with the details of the program name and resources that the program uses. You can set **Performance Alerting** to the **On**,

	Log Only, or the **Off** mode. The **Details & Settings** link in the notification alert lets you view additional details about the resource consumption by the program in the **File Insight** window. ▪ **Resource Threshold Profile for Alerting** Lets you configure the resource threshold profile for displaying performance alerts. ▪ **Use Low Resource Profile On Battery Power** Lets you configure Norton Internet Security to change the resource threshold to low profile when your computer runs on battery power.

	▪ **Alert for High-Usage of:** ▪ **CPU** When this option is turned on, Norton Internet Security detects and notifies you with the details of increased usage of the CPU resource by any program or process. ▪ **Memory** When this option is turned on, Norton Internet Security detects and notifies you about the increased usage of memory by any program or process. ▪ **Disk** When this option is turned on, Norton Internet Security detects and notifies you about the increased usage of your disk by any program or process. ▪ **Handles** When this option is turned on, Norton Internet Security detects and notifies you

	about the increased usage of handles by any program or process. ▪ **Program Exclusions** Lets you select specific programs to exclude from appearing in performance alerts.

Product Security	

	Lets you protect Norton Internet Security from unauthorized changes. Your options are: **Non-Admins Access to Settings** Lets you access and configure all the options in the **Settings** window from a non-admin user account as well. By default, this option is turned off. You need to log in to your computer as an administrator to turn on this option. You cannot access the **Settings** window if the Settings window is opened in some other user account on your computer. **Norton Product Tamper Protection** Lets you protect your Norton product from an attack or modification by unknown or suspicious applications. **Settings Password Protection** Lets you set up a password to protect Norton Internet Security settings. It protects the product settings from unauthorized access. If you set a password, you must enter the password each time that you want

	to view or configure your product settings. However, if you forget your settings password, you can reset the password in the window that appears when you choose to uninstall Norton Internet Security. You do not need to uninstall the product to reset your password. You can use the **reset settings password** option in the uninstall preference window to reset your password.

Silent Mode Settings	

Lets you turn on or turn off **Silent Mode**.

Your options are:

- **Silent Mode**

  When you turn on the **Silent Mode** option, Silent Mode is enabled for a specified duration. Norton Internet Security suppresses all alerts and suspends the background activities for the duration that you specify.
- **Full Screen Detection**

  When you turn on the **Full Screen Detection** option, Norton Internet Security automatically detects the applications that are run in full-screen mode and enables Silent Mode. Norton Internet Security suppresses most of the alerts and suspends the background activities. The only activities that run are those that protect your computer from viruses and other security threats.
- **Quiet Mode on Detection of:**
  - **IMAPI 2.0 Disk Burn**

    When you use the Media Center application to burn a CD or DVD, Norton Internet Security detects the activity, and automatically

	turns on Quiet Mode. When Quiet Mode is turned on, Norton Internet Security suppresses the background activities but continues to display alerts and notifications. ▪ **Media Center TV Recording** When you use the Media Center application to record a TV program, Norton Internet Security detects the activity, and automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton Internet Security suppresses the background activities but continues to display alerts and notifications.

	▪ **User-Specified Programs** When you run an application that is listed in the User-Specified Programs list, Norton Internet Security detects the activity, and automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton Internet Security suppresses the background activities but continues to display alerts and notifications. You can configure the list of programs for which you want to turn on Quiet Mode.

About Norton Product Tamper Protection

Norton Product Tamper Protection prevents outside programs from making changes to the Norton product. This security feature also prevent Windows System Restore from changing Norton files, which results in the **Restoration Incomplete** message.

Norton Product Tamper Protection protects Norton Internet Security from an attack or modification by any virus or other unknown threat. You can protect your product from accidental modification or deletion by keeping the **Norton Product Tamper Protection** option turned on.

If you want to temporarily turn off **Norton Product Tamper Protection**, you can turn it off for a specified duration.

You cannot run System Restore on your computer when **Norton Product Tamper Protection** is turned on. You must temporarily turn off **Norton Product Tamper Protection** to run a successful System Restore.

Turning off or turning on Norton Product Tamper Protection

Norton Product Tamper Protection protects the Norton Internet Security files from an attack or modification by any virus or other unknown threat. You can protect your product from accidental modification or deletion by keeping the **Norton Product Tamper Protection** option turned on.

If you want to temporarily turn off **Norton Product Tamper Protection**, you can turn it off for a specified duration.

You cannot run System Restore on your computer when **Norton Product Tamper Protection** is turned on. You must temporarily turn off **Norton Product Tamper Protection** to run a successful System Restore.

To turn off Norton Product Tamper Protection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Product Security**.
4. In the **Norton Product Tamper Protection** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **Apply**.
6. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Norton Product Tamper Protection.
7. Click **OK**.
8. In the **Settings** window, click **OK**.

To turn on Norton Product Tamper Protection

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Product Security**.
4. In the **Norton Product Tamper Protection** row, move the **On/Off** switch to the left to the **On** position.
5. Click **Apply**, and then click **OK**.

About securing Norton Internet Security Settings using a password

You can configure Norton Internet Security to prevent unauthorized access to your product settings. If you share your computer with others and do not want them to modify your Norton Internet Security Settings, you can secure Norton Internet Security Settings using a password. The **Settings Password Protection** option lets you secure your Norton Internet Security Settings by setting up a password.

By default, **Settings Password Protection** option is turned off. You must turn on the **Settings Password Protection** option to set up a password for your product settings. To use the **Settings Password Protection** option, go to the Norton Internet Security main window, and then click **Settings >General >Product Security**. The password must be between 8 and 256 characters in length.

After you set up a password for Norton Internet Security Settings, you must enter the password each time to access or configure your product settings. If you forget your settings password, you can reset the password in the window that appears when you choose to uninstall Norton Internet Security. You do not need to uninstall the product to reset your password. You can use the **reset settings password** option in the **Select your Uninstall Preference** window to reset your password.

The **reset settings password** option appears in the **Select your Uninstall Preference** window only when the **Settings Password Protection** option is turned on.

You can turn off the **Settings Password Protection** option if you no longer require password protection for your Norton Internet Security Settings.

Securing your Norton Internet Security Settings using a password

You can secure your Norton Internet Security Settings from unauthorized access by setting up a password for your product settings. The Settings Password Protection option lets you secure your Norton Internet Security Settings using a password.

After you set up a password for Norton Internet Security settings you must enter the password each time to view or configure your product settings.

By default, the **Settings Password Protection** option is turned off. You must turn on the **Settings Password Protection** option to set up a password for your product settings.

The password must be between 8 and 256 characters in length.

To secure your Norton Internet Security Settings using a password

1. In the Norton Internet Security main window, click **Settings**.
2. In the **Settings** window, click the **General** tab.
3. In the left pane, click **Product Security**.
4. In the **Settings Password Protection** row, move the **On/Off** switch to the left to the **On** position.
5. Do one of the following:
   - In the **Settings Password Protection** row, click **Configure**.
   - In the **Settings** window, click **Apply**.

6 In the dialog box that appears, in the **Password** box, type a password.
7 In the **Confirm Password** box, type the password again.
8 Click **OK**.
9 In the **Settings** window, click **OK**.

Turning off Norton Internet Security Settings password

You can protect your Norton Internet Security Settings with a password using the **Settings Password Protection** option. If the **Settings Password Protection** option is turned on, you need to enter the Settings password each time to view or configure your Norton Internet Security settings. You cannot access the product settings without providing your Settings password.

In case you forget your Settings password, you can reset it using the **reset settings password** option in the **Select Uninstall Preference** window.

You can turn off the **Settings Password Protection** option if you do not require password protection for Norton Internet Security settings.

To turn off Norton Internet Security Settings password

1 In the Norton Internet Security main window, click **Settings**.
2 In the dialog box that appears, in the **Password** box, type your Settings password, and then click **OK**.
3 In the **Settings** window, click the **General** settings tab.
4 In the left pane, click **Product Security**.
5 Click **Apply**, and then click **OK**.

Resetting your Norton Internet Security Settings password

If you forget your Norton Internet Security Settings password, you can reset the password. You can reset

your Norton Internet Security Settings password using the **reset settings password** option in the **Select Uninstall Preference** window.

To access the **Select Uninstall Preference** window, you must choose to uninstall Norton Internet Security. However, you need not uninstall the product to reset your Settings password.

The **reset settings password** option appears in the **Select Uninstall Preference** window only if the **Settings Password Protection** option is turned on. To use the **Settings Password Protection** option, go to the Norton Internet Security main window, and then click **Settings >General >Product Security** .

To reset your Norton Internet Security Settings password

1. On the Windows taskbar, click **Start** > **Control Panel**.
2. In **Windows Control Panel**, do one of the following:
   - In Windows XP, double-click **Add or Remove Programs**.
   - In Windows Vista, click **Programs and Features**.
   - In Windows 7, click **Programs** > **Programs and Features**.

     The **Programs** option in Windows 7 is available when you select the **Category** option in the **View by** drop-down list.
3. In the list of currently installed programs, do one of the following:
   - In Windows XP, click **Norton Internet Security**, and then click **Change/Remove**.
   - In Windows Vista or Windows 7, click **Norton Internet Security**, and then click **Uninstall/Change**.
4. At the bottom of the **Select Your Uninstall Preference** window, click **reset settings password**.

5 In the dialog box that appears, in the **Reset Password Key** box, type the randomly generated key that is displayed against **Reset Password Key**.
6 In the **New Password** box, type the new password.
7 In the **Confirm New Password** box, type the new password again.
8 Click **OK**.

Finding additional solutions

9

This chapter includes the following topics:

- Finding the version number of your product
- Finding the End-User License Agreement
- About upgrading your product
- About Norton Autofix
- Staying informed about protection issues
- About Support
- About uninstalling

Finding the version number of your product

If you want to upgrade your Norton product or want to reach the customer support for assistance, you must know your product version number. You can find the version number of your product on your computer.

To find the version number of your product

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, move your mouse pointer over **About**.
   You can note the version number of your product in the dialog box that appears.

Finding the End-User License Agreement

End-User License Agreement (EULA) is a legal document that you agree to while installing the product. EULA contains information such as the restriction on sharing or usage of the software, the user rights on the software, and the support information.

You can read the EULA to learn more about the following information:

- The usage policies of Norton Internet Security.
- The terms and conditions for using Norton Internet Security.

To find the End-User License Agreement

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, click **User License Agreement**.
3. Read the Norton License Agreement and click **Close**.

About upgrading your product

Norton Internet Security helps you upgrade your product if you have an active subscription. You can upgrade your current product to the latest version without any cost as long as you have an active subscription with the current product. You can access this option from the **Support** drop-down menu in the Norton Internet Security main window. If a new version of your product is available, Norton Internet Security lets you download the new version.

The **Automatic Download of New Version** option automatically downloads the latest available version of Norton Internet Security and prompts you for free installation. To get the latest version of Norton Internet Security, you need to turn on the **Automatic Download of New Version** option. To turn on the **Automatic**

Download of New Version option, go the Norton Internet Security main window, and then click **Settings > Updates > Automatic Download of New Version > On**.

If you choose to install the latest version of the product, Norton Internet Security downloads and seamlessly installs the latest version. Ensure that you have saved all your important data such as pictures and financial records before you install the new version of the product.

If you download and install the latest version of your product, your subscription status remains the same as your previous version of product. For example, you have 200 days of subscription left with your current version of product and you upgrade your product to the latest version. In this case, the subscription status of your upgraded product remains 200 days only.

If a new version is not available, the Web page informs you that no new version is available and your product is up to date. Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats.

Product upgrade is different from the program updates and the definition updates that are minor improvements to your installed product. The main differences are as follows:

- Product upgrade lets you download and install a new version of the entire product.
- Definition updates are the files that keep your Symantec products up to date with the latest antithreat technology.
- Program updates are enhancements to Norton Internet Security that Symantec issues periodically.

If a new version of the product is not available, ensure that you have all the latest program updates and definition updates. LiveUpdate automates the process of obtaining and installing program and definition

updates. You can use LiveUpdate to obtain the latest updates.

The upgrade process might not work if your Web browser is incompatible to communicate with the Symantec servers.

Your product must be activated and you need an Internet connection to check and install new product version.

Checking for a new version of the product

You can upgrade your product to the latest version if you have an active subscription. If you have a new version available, you can download and install the new version of your product. You can also let Norton Internet Security notify you when a new version of your product is available. You can do so by turning on the **Automatic Download of New Version** option. To turn on the **Automatic Download of New Version** option, go the Norton Internet Security main window, and then click **Settings > Updates > Automatic Download of New Version > On**. The latest version of your product may contain new and enhanced features for better protection against security threats.

When you check for a new version, details about your product such as product name and version are sent to Symantec servers. The servers then check whether a new version of the specified product is available or not.

If a new version is available, you can download and install it from the Web page. If a new version is not available, the Web page informs you about it. In such case, you can run LiveUpdate to obtain latest program and definition updates and keep the existing version of your product up to date.

The upgrade process might not work if your Web browser is incompatible to communicate with the Symantec servers. You can use Internet Explorer versions 5.5 or later and Firefox versions 3.0 or later.

Your product must be activated and you need an Internet connection to check if a new version is available and install new version of the product.

To check for a new version of the product

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, click **New Version Check**.
   This option is available only if your product is activated. The Web page that appears displays whether a new version of the product is available or not.
3. Follow the on-screen instructions to download the new product.

About Norton Autofix

Norton Autofix provides additional product support with one-click access from the Norton Internet Security main window. Norton Autofix performs a Quick Scan of your computer and repairs problems without your intervention. If the problem persists, you can use the **Open Support Web Site** option to go to the Norton Support Web site for help by telephone, email, chat, or forum.

In addition, the Norton Support Web site provides access to the knowledge base articles. By using these articles, you can easily find solutions to your technical problems.

The support technicians can help you solve more complex problems by using remote-assistance technology.

Support offerings can vary based on the language or product.

When you click the **Get Support** option in the **Support** drop-down menu, Norton Internet Security checks your Internet connection. To access Norton Autofix, ensure

that your computer is connected to the Internet. If you use a proxy server to connect to the Internet, you must configure the proxy settings of Norton Internet Security. See "Configuring Network Proxy Settings" on page 62.

If you do not know your proxy settings, contact your Internet service provider or network administrator for assistance.

Solving a problem using Norton Autofix

Norton Autofix performs a Quick Scan of your computer and repairs problems without your intervention. If a problem persists, you can use the Norton Support Web site for additional online support and contact options.

Your computer must be connected to the Internet to access Norton Autofix. If you use a proxy server to connect to the Internet, you must configure the proxy settings of Norton Internet Security.

If you do not want to proceed with the support session, you can use the **Skip** option to bypass the scan.

To solve a problem if your computer is connected to the Internet

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. In the **Norton Autofix** window, do one of the following:
   - If the problem is not fixed automatically, click **Open Support Web Site**, and follow the on-screen instructions to find additional support.
   - If the problem is fixed, click **Close**.

To solve a problem if your computer is unable to connect to the Internet

1. In the Norton Internet Security main window, click **Support**.

2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions in the **Checking Your Connection** window to attempt to correct your connection issue.
4. In the **Checking Your Connection** window, click **Retry**.
5. If you use a proxy server to connect to the Internet, you may be prompted to authenticate. If you are prompted, then in the **Proxy Settings Detected** window, do the following:
   - In the **Username** box, type the user name that you provided when you configured your Network Proxy settings.
   - In the **Password** box, type the password that you provided when you configured your Network Proxy settings.
   - Click **OK**.
6. If the problem still persists, in the **Norton Autofix** window, click the **click here** link.
   Under **Support Contact Numbers**, select the region, and then your country to view the contact details. You can use the contact details to contact the technical support team.

Staying informed about protection issues

If you need help using Norton Internet Security, you can find helpful information on the Symantec Web site. It contains many useful and informative features that are especially designed to complement Norton Internet Security, including the following:

- Detailed background information about current threats and outbreaks.
- Newsletter to which you can subscribe.
- Protection blog that lets you post your own comments and view comments from experts.

The Symantec Web site is constantly updated and enhanced, so the available resources may vary.

To stay informed about protection issues

1. Open your Web browser, and go to the following URL:
   http://www.symantec.com
2. In the **Symantec** Web site, click **Norton**.
3. In the menu that appears, do the following:
   - Click the **Viruses & Risks** tab, and then click any item on the left pane to find out more details about it.
   - Click the **Community** tab, and then use one of the following:

Norton Forums	Register as a user and participate in discussions. You can create your own threads of topics or take help from the existing forum discussions.
Norton Blogs	Read the messages that prominent leaders post from inside and outside Symantec and obtain information straight from the source. You can add comments or ask questions on the blogs that you are interested in.
Other Norton Communities	Check about Norton in other Web sites and social networks that are available.

About Support

If you have purchased Norton Internet Security, you can access Support from the product.

Support offerings may vary based on the language or product.

About Norton Support Web site

The Norton Support Web site provides a full range of self-help options.

By using Norton Support Web site, you can do the following:

- Find help with your product download, product subscription, product activation, product installation, and other issues.
- Find and download the latest product manual.
- Manage your products and services using Norton Account.
- Search Norton Forum to find the additional product help about installing, configuring, and troubleshooting errors. You can also post your questions in the forum and get answers from experts. To post your questions, you need to first register for Norton Forum.
- Find information about the latest virus threats and removal tools.

Availability of support varies by region, language, or product. For additional support, go to the following URL:

www.symantec.com/globalsupport

In addition to the self-help options, you can use the **Contact Us** option at the bottom of the Web page to

contact the technical support team in the following ways:

Chat	Chat in real time with a support representative. For more complex technical issues, chat offers the option to allow a support representative to connect remotely to your computer and resolve your problem.
Email	Submit your question on our Web site and receive a response by email. Email support has a slower response time than chat or phone.
Phone	Speak to a support representative in real time.
Forum	Search for additional product help about installing, configuring, and troubleshooting errors.

Using the Norton Support Web site

Norton Support Web site contains answers to the most common customer questions. You can find the latest product manual, knowledge base articles, and virus removal tools.

Norton Support Web site contains problem-solving articles that are presented in an easy step-by-step format. The articles are categorized and listed on the left side of the Web page. Using the categories, you can browse through the available support topics. You can

also use the **Search Support** box to find solution using a keyword.

Norton Support Web site also contains useful links to the product manual, the Norton Account, the Norton Forum, and the spyware help under **Additional Resources**.

To use the Norton Support Web site

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions.
4. In the **Norton Autofix** window, click **Open Support Web Site**.
   The Norton Support Web page appears.
5. Follow the on-screen instructions.

About phone support

If you have a problem that you cannot resolve using Norton Autofix, use the **click here** link on the **Norton Autofix** window to get the phone number to contact a support representative.

Support offerings may vary based on the language or product.

If you cannot access phone support by using Norton Autofix, then you can access the phone support options at the following URL:

http://www.symantec.com/globalsupport

Getting support by phone

When you click the **Get Support** option in the **Support** drop-down menu, Norton Autofix performs a Quick Scan of your computer and should repair your computer problems. However, if the problem persists, you can use the **Open Support Web Site** option to go to the Norton Support Web site for help by telephone, email, chat, or forum.

You can also use the **click here** link at the bottom of the **Norton Autofix** window to contact a support representative.

Availability of support varies by region. Regular telephone and Internet connection fees apply in certain countries.

To get support by phone

1. In the Norton Internet Security main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions.
4. At the bottom of the **Norton Autofix** window, click the **click here** link.
5. In the **Norton Autofix** window, under **Support Contact Numbers**, select the region, and then the location.
   You can use the phone number to contact a support representative.

Support policy

Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats. In case of older versions, complimentary support is offered for a minimum of 2 years. However, technical information on these products may still be available through the support Web site at the following address:

www.symantec.com/globalsupport

Symantec reserves the right to change its support policies at any time without notice. You can view the latest version of the support policy at the following URL:

www.symantec.com/supportpolicy

About keeping your subscription current

Subscription period lengths vary by Symantec product. To maintain uninterrupted protection, you must keep your subscription up to date. If you do not renew your subscription, you cannot obtain updates of any kind and the software no longer functions.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Follow the on-screen instructions to renew your subscription.

When you renew your subscription, the definition updates and new product features are available throughout the subscription period. Please note that features may be added, modified, or removed during this period.

Worldwide service and support

Worldwide service and support solutions vary by country. To contact one of our Support offices, please go to the following Web site and select your language.

www.symantec.com/globalsupport

ClubNorton

ClubNorton is your one-stop resource center for Internet security. As a Norton customer, Symantec wants to make your experience with your computer safe, enjoyable, and productive. Whether you use your computer to manage your personal finances, shop online, or share your latest digital photos with friends and family, ClubNorton makes your experience a good one. Our goal is to consistently provide the proper tools and information to keep you up to date.

For more information, go to the following URL and select your country or region in the **Select Your Country/Region** drop-down menu:

www.clubnorton.com

The ClubNorton Web page includes a regularly updated article library, a glossary, the Norton Forums, and the Norton Update Center. You can also find the following useful links in the Web page:

- Symantec Security Check
- Subscription Troubleshooter
- Home & Home Office Security
- Product Manuals
- Product Updates
- Product Reviews
- Order Status
- Returns
- Rebates

About uninstalling

To remove your Symantec product from your computer, use the **Add/Remove Programs** option in the Windows **Control Panel**.

You must restart your computer after uninstalling the product, so ensure that you do not have any other programs running while you follow this procedure.

Uninstalling Norton Internet Security

You can remove Norton Internet Security in the following ways:

- From Windows **Control Panel**.
- From the **Start** menu.

You cannot access online Help while uninstalling. Therefore, you should print out the Uninstalling Norton Internet Security Help topic before continuing to uninstall.

You may need to uninstall Norton Internet Security for some purpose. You can reinstall the product using the installation file that you downloaded from

Symantec Web site or from the CD. To reinstall Norton Internet Security, follow the installation procedures that are available in the user guide.

During uninstallation, Norton Internet Security offers to leave the Norton Toolbar for free to search and browse safely over the Internet even after the product is uninstalled. You can choose to keep the Norton Toolbar that comprises Norton Safe Search and Norton Safe Web features without any cost. Norton Safe Search provides site safety status and Norton rating for each of the search results generated. Norton Safe Web analyses the security levels of the Web sites you visit and indicates if the Web sites are free from threats.

Your computer must be connected to the Internet to avail this option. Norton Internet Security does not offer to leave the Norton Toolbar if you upgrade your product to the latest version or choose to reinstall another Norton product.

To uninstall Norton Internet Security from Windows Control Panel

1. On the Windows taskbar, click **Start > Control Panel**.
2. In Windows **Control Panel**, do one of the following:
   - In Windows XP, double-click **Add or Remove Programs**.
   - In Windows Vista, click **Programs and Features**.
   - In Windows 7, click **Programs > Programs and Features**.

     The **Programs** option in Windows 7 is available when you select the **Category** option in the **View by** drop-down list.
3. In the list of currently installed programs, do one of the following:
   - In Windows XP, click **Norton Internet Security**, and then click **Change/Remove**.
   - In Windows Vista or Windows 7, click **Norton Internet Security**, and then click **Uninstall/Change**.

4 In the page that appears, under **Select Your Uninstall Preference**, click one of the following:

I plan to reinstall a Norton product in the future. Please leave my settings behind.	Lets you retain your settings, passwords, and preferences for Norton features before you uninstall Norton Internet Security. Select this option if you want to reinstall Norton Internet Security or another Norton product.
Please remove all user data including my stored passwords & quarantine contents.	Lets you completely remove Norton Internet Security without saving your settings, passwords, and preferences.

5 If Norton Internet Security offers to install the Norton Toolbar after uninstall, do one of the following:

- To keep the Norton Toolbar after uninstall, click **Agree**.
- To uninstall Norton Internet Security without keeping the Norton Toolbar, click **No**.

6 To uninstall Norton Internet Security, click **Next**.

7 Do one of the following:

- Click **Restart Now** (recommended) to restart the computer.
- Click **Restart Later** to restart the computer later.

Norton Internet Security is not fully uninstalled until you restart your computer.

To uninstall Norton Internet Security from the Start menu

1 On the Windows taskbar, do one of the following:
- In Windows XP, click **Start > Programs > Norton Internet Security > Uninstall Norton Internet Security**.
- In Windows Vista or Windows 7, click **Start > All Programs > Norton Internet Security > Uninstall**.

2 In the page that appears, under **Select Your Uninstall Preference**, click one of the following:

I plan to reinstall a Norton product in the future. Please leave my settings behind.	Lets you retain your settings, passwords, and preferences for Norton features before you uninstall Norton Internet Security. Select this option if you want to reinstall Norton Internet Security or another Norton product.
Please remove all user data including my stored passwords & quarantine contents.	Lets you completely remove Norton Internet Security without saving your settings, passwords, and preferences.

3 If Norton Internet Security offers to install the Norton Toolbar after uninstall, do one of the following:
- To keep the Norton Toolbar after uninstall, click **Agree**.
- To uninstall Norton Internet Security without keeping the Norton Toolbar, click **No**.

4 To uninstall Norton Internet Security, click **Next**.

5 Do one of the following:

- Click **Restart Now** (recommended) to restart the computer.
- Click **Restart Later** to restart the computer later.

Norton Internet Security is not fully uninstalled until you restart your computer.

See "About uninstalling" on page 486.

Index

A

about customer support 481
accessing
  Facebook Scan 115
accessing Norton Internet Security scans
  Computer Scan 115
  Reputation Scan 115
Actions window
  deleting security risks 387
  performing actions 387
  restoring security risks 387
  submission, items to Symantec 387
activation
  about 13
  alerts 14
  Norton Account 33
  problems 17
  procedure 14
  troubleshooting 17
Add Rule Wizard
  opening 204
  using 205
Address Book Exclusions
  setting 260
addresses
  adding allowed 261
  adding blocked 263
  importing allowed 261
Advanced Mode
  allow an event 157
adware
  about 254
  found by Auto-Protect 181
  in freeware programs 254
  protection features 411
Aggressive
  SONAR Protection 157
alerts
  responding to 197
  Worm Blocking 186
Allowed List 261
Antiphishing
  about 302
  hiding the toolbar 360
  showing the toolbar 360
  turning off 304
  turning on 304
AntiSpam
  about 255
  Address Book Exclusions 260
  Allowed List 261
  Blocked List 263
  Client Integration 258
  configure 257
  Feedback 266
  settings 257
  Web Query 267

Antispyware
managing using the main window 255
Application Ratings
check trust level 99
Scan Performance Profiles 101
attack signatures 244
attacks
network 194
attention
infected files 188
infected items 122
resolve any items 122
Attention Required
about 122
resolving the risk 122
Auto-Protect
functions 407
notifications 181
turning on and off 416
automatic features
disabling 416
Automatic LiveUpdate
turning off or turning on 57
Automatic Program Control
about 197
turning on and off 199

B

background jobs
about 88
monitoring 89
backup
Identity Safe data 348
Backup and Restore
about 348
Bandwidth
defining usage 299
managing 297
Blocked List 263
blocking
spam 255
Boot Time Protection 176
configure 177

C

Cards
about 342
adding 343
deleting 344
duplicating 344
update image 343
updating 344
changing
scan schedules 131
Client Integration
configuring 258
cloud technology
Cloud 134
ClubNorton
security tips 485
communication port
modifying 296
computer
protection status 32
Computer Settings
about 428
computers
blocking with AutoBlock 247
IP address 284
configure
Identity Safe 328
CPU graph
about 78
obtaining historical data 80
resource-consuming processes 81
CPU usage
viewing 79
Creating custom scans
adding files 123

Creating custom scans *(continued)*
adding folders 123
Crimeware Protection
turning off or turning on 420
custom scan
configure scan options 125
select items 124
custom scans
about 123
creating 123
deleting 127
editing 126
particular area 123
running a custom scan 126
scan frequently 123
schedule the custom scan 123
scheduling 128, 131
customer support
about 481
using 482
customizing
Allowed List 261
Blocked list 263

D

definition status 56
definition updates 50
obtaining 59
deleting
custom scans 127
deleting custom scans
deleting 127
detecting
security risks 180
device
adding 282
editing details 285
excluding from Intrusion Prevention scan 291
purging from exclusion list 250
remotely monitoring 274
device *(continued)*
removing from the Network Security Map 293
viewing 274
devices
changing trust level 287
domains
adding allowed 261
adding blocked 263
Download Insight
about 233
configuring alerts 240
turning off notifications 238
turning on notifications 238
Download Intelligence
turning off 237
turning on 237

E

email
menu 265
program 265
spam 255
emergency
preparations 107
ensuring
protection settings 108
EULA
checking 474
Events graph
monitoring activities 68

F

features 407
email filtering 413
security protection 412
security risk protection 411
Feedback
Norton AntiSpam 266

file extensions
of infected files 188
filter
Web Query 267
filtering
email 257
identifying email senders 261, 263
SSL 255
web-based 267
firewall rules
about 194
adding 204
changing the order of 214
creating 197, 205
default 195
modifying 212
processing order 195, 214
removing 216
turning on and off 215
Full Screen Detection
about 163
Full System Scan
running Full System Scan 118
scheduling 130

G

General Rules
adding 204
changing 212
removing 216
turning on and off 215

H

high-risk security threats
excluding from scanning 159

I

Identity Safe
about 313
Identity Safe *(continued)*
accessing 326, 360, 364
backing up 349
changing password 355
configuring 328
information 301
logging in and out 327
logins 332
Norton toolbar 327
options 351
password 352
restoring data 350
security 352
turning off or turning on 420
Identity Safe Options
about 351
Identity Safe Password & Security options
about 352
Identity Safe profiles
about 317
creating 318
identity theft
Internet 301
Idle Time Optimizer
about 86
turning off 87
turning on 87
Idle Time Out
setting 156
Idle Time Scans
about 153
Full System Scan 153
Quick Scan 153
turning off 155
turning on 155
import
logins 324
Insight Network
about 134
cloud computing 134

Insight Network *(continued)*
Insight Network scan 134
Quick Scan 134
scan 134
shortcut menu scan 134
Single File Scan 134
Insight Protection
turning off 136
turning on 136
installation
problems 43, 45
Instant Messenger
virus protection 407
integration with email clients 258
integration with email programs 265
Intrusion AutoBlock
blocking computers permanently 249
turning on and off 247
unblocking computers 248
Intrusion Prevention
about 244, 412
exclusion list 249
turning individual notifications on and off 245
turning notifications on and off 245
turning on and off 419
Intrusion Prevention scan
excluding a device 291
exclusion list 249
purging devices 250
remove devices 250
IP addresses 284
finding 284
items
submitting from Quarantine 405

K

keystroke logging 254, 411

L

LiveUpdate
about 49
Smart Definitions 52–53
using 55
when to run 54
Login
adding manually 335
changing password 340
changing URL 338
changing user name 340
configuring 328
creating new folder 335
deleting 335
editing 335
importing 324
managing 335
saving 333
updating 341
low resource profile on battery
turning off 76
turning on 76

M

main window
options 17
maintaining protection
about 107
avoiding security risks 107
Manage Logins
about 332
Manage Notes
about 346
Manual Repair
reviewing remaining risks in 188

Manual Repair window
reviewing remaining risks in 118, 120
Media Center Extender
Silent Mode 167
Memory graph
about 78
obtaining historical data 80
Metered Broadband Mode
about 297
turning off 298
turning on 298
Metered Broadband mode
defining bandwidth 299
Miscellaneous Settings
about 446
Monthly Report
about 103
viewing 104

N

Network
changing trust level 287
discovering devices 280
editing details 286
forming 280
joining 280
managing 272
Network Proxy Settings
about 60
configuring 62
Network Security Map
about 272
adding devices 282
modifying communication port 296
purging 293
removing devices 293
turning off 281
turning off Network Security Overview 273
Network Security Map *(continued)*
turning on Network Security Overview 273
viewing device details 295
viewing devices 274
wireless network
viewing status 294
Network Security Overview
turning off 273
turning on 273
Network Settings
about 435
new version
checking 476
newsletter 485
non-admin account 422
Norton Account
about 33
accessing 38
creating 37
Norton AntiSpam 255
about 255
Address Book Exclusions 260
configure 257
Feedback 266
settings 257
SSL 255
Web Query 267
Norton Bootable Recovery Tool
about 41
using 45
Norton Bootable Recovery Tool Wizard
downloading 43
Norton Community Watch
about 39
joining 39
turning off or turning on 418
Norton Firewall Diagnosis
about 232

Norton Insight
about 92
Files of Interest 96
refreshing trust level 96
trusted files 92
viewing processes 96
Norton Internet Security
about securing 467
activating 14
Allowed and Blocked lists 413
background jobs 88
EULA 474
icon 46
main window 17
new version 476
password 468–469
protecting 469
registering 37
securing 468
settings 423, 435
shortcut menu 48
starting from the DOS command prompt 46
uninstalling 486
upgrading 474
version number 473
Norton Internet Security scan
about 110
accessing Norton Internet Security scans 115
command line scanning 132
Computer Scan 110
custom scans 123
Full System Scan 118
Idle Time Scan 110
Insight Network 134
Insight Network scan 110
Quick Scan 119
Reputation Scan 110
Norton Internet Security settings
resetting password 469
Norton LiveUpdate
about 49
obtaining updates 55
Norton Product Tamper Protection
about 465
turning off 466
turning on 466
Norton Safe Search
searching Web 310
Norton Safe Web
about 305
Scan Facebook Wall 150
scanning 152
turning off 312
turning on 312
Norton Tasks
about 88
Norton toolbar
about 356
accessing 360
settings 326
Notes
deleting 347
saving 347
updating 347
notification area
icon 46
shortcut menu 48
notifications
Auto-Protect 181
Intrusion Prevention 245

O

Office documents
embedded objects 161
scanning office documents 161
turn on or turn off 162
virus macros 161
One Click Support
support assistants 477
using 478

Online transactions
identity theft 313
Optimization
about 84
boot volume 85
Options
Client Integration 258
customizing 422
password protection 407
Smart Firewall 217
Smart Firewall Advanced Settings 220
Smart Firewall Program Control 218
Smart Firewall Trust Control 219

P

Parental Control
settings 414
password
changing 355
editing 335
for Settings 423
saving 333
updating 341
PC Tuneup
Startup Manager 81
Performance
accessing 67
alerts 71
monitoring 79
performance alerts
about 71
configure 72
configure threshold 74
excluding programs 77
removing programs from exclusion list 77
turning off 72
performance alerts *(continued)*
turning off low resource profile 76
turning on 72
turning on low resource profile 76
Personal data
backing up 349
Personal Firewall
about 412
turning on and off 419
Phishing Protection
turning off or turning on 420
port scans 194
preparing for emergencies
maintaining protection 107
problem solving 479
problems
problems found during 188
resolve any items 188
solving 478
Product Key 15
accessing 38
product password
protecting 468
product status 56
program
patches 50
Program Control
adding programs 200
Automatic 197
customizing 203
options 218
removing programs 202
turning on and off 199
Program rules
adding 204
changing 212
removing 216
program updates 50

programs
adding to Program Control 200
configuring Internet access 204
creating firewall rules 204
removing from Program Control 202
protection
preparing for emergencies 107
system scans 118
protection settings
configuring 108
ensuring 108
turning on 108
proxy server
configuring 62
settings 60
Pulse Updates
about 59
using 59

Q

Quarantine
adding an item 403
items, submitting for analysis 405
managing items 401
opening 401
restoring items 404
Quarantined Items view
adding items 374
Quick Scan 407
scheduling 130
Quiet Mode
about 163, 169
disk burning 169
options 172
turning off 172
turning on 172
TV recording 169
User-Specified Programs 174

R

Real Time Exclusions
about 158
Remote Monitoring
setting up 280
repair
actions 188
infected files 188
removable media 188
system files 188
repairing
viruses 407
Reputation Scan
about 137
results 143
running Custom Scan 142
running Full System Scan 141
running Quick Scan 142
restore
Identity Safe data 348
restoring items
Quarantine 404
result
resolved risks 121
Results Summary
about 121
resolved risks 121
total items scanned 121
risks
intrusions 194
port scans 194
rules
changing 205, 212
creating 204–205
Running custom scans
scanning required files 126
scanning required folders 126
running Full System Scan
Reputation Scan 141
scanning entire computer 118

running Quick Scan
fast scan 119
Insight Network Quick Scan 119
Quick Scan 119
Reputation Scan 142

S

Safe Surfing
about 301
Safe Web
turning off 312
turning on 312
scan at the command prompt
command line scanning 132
Scan Complete
appearing after a scan 188
Scan Complete window
appearing after a scan 118, 120
Scan Facebook Wall
about 150
scanning 152
scanned
total items scanned 121
scanning
automatically 128
entire computer 118
individual elements 120
problems found during 188
Scans
command line 132
Computer Scan 116
create a custom scan 123
Custom Scan 116
deleting custom scans 127
file 120
floppy disk 120
folder 120
Full System Scan 116
hard drive 120
Insight Network 134
Scans *(continued)*
Norton Bootable Recovery Tool 45
Quick Scan 116
removable drive 120
running custom scans 126
using custom 123
scheduling
custom scans 128
scans 128
scheduling custom scan
multiple schedules 128
scheduling custom scans
scheduling Full System Scan 128
searching
Security History 398
Security History
about 371
Actions window 387
adding items to the Quarantine 374
firewall alerts 374
full alert history 374
importing or exporting 399
manual scan results 374
network alerts 374
opening 373
Quarantine 401
Quick Search 398
recent alert history 374
searching 398
security risks 374
submission, items to Symantec 374
suspicious email 374
traffic alerts 374
viewing items 374
viewing quarantined items 374
security protection
about 412

security risks
about 254, 411
adding to Quarantine 403
assessment 411
attacks 194
found by Auto-Protect 179, 181
managing protection using the main window 254
other programs 254
port scans 194
protection features 411
restoring 411
restoring from Quarantine 404
scan 411
security status indicator
viewing 32
self-healing 477
Settings
accessing 423
configuring 423
customizing 422
Miscellaneous 446
settings password
resetting 469
turning off 469
Settings Password Protection
about 467
configuring 468
resetting 469
turning off 469
Signature Exclusions
about 160
Signature Ezclusions
excluding items 160
signatures
including and excluding 246
Silent Mode
about 163
Full Screen Detection 167
Media Center Extender 167
turning off 165, 168
Silent Mode *(continued)*
turning on 165, 168, 446
turning on manually 165
Smart Definitions
about 52
turning on or turning off 53
Smart Firewall
about 193
customizing 194
options 220
SONAR Protection
about 157
emerging threats 157
heuristic technology 157
SONAR Advanced Mode 157
turning off 157
turning on 157
spyware
about 254
found by Auto-Protect 181
managing protection using the main window 254
protection features 411
SSL (Secure Sockets Layer)
Norton AntiSpam 255
starting
spam blocking 417
virus protection 407
startup files 180
startup items
delaying and running 83
disabling or enabling 82
Startup Manager
about 81
delaying and running delayed items 83
disabling or enabling startup items 82
stopping spam blocking 417
submission, items to Symantec 405

subscription
maintaining 485
product updates 56
summary
product features 407
Supervisor user account
creating firewall rules 197
Support
AutoFix Scan 478
Self Help 481
solving problems 478
worldwide service 485
Support policy 484
Symantec Security Response 405
viewing submitted files 374
Symantec Support Web site
about 481
using 482
Symantec Web site
blogs and forums 479
System Insight
about 65
Events graph 65
monitoring activities 68
Performance graph 65
system status graph
activity details 70
System Status indicators
responding 31

T

technical support
about 481
using 482
threats
avoiding 107
newly discovered 56
protection from 193
Trust Control
about 412
Intrusion Prevention and 244
Trust Control *(continued)*
options 219
trust level
changing 287
device 287
network 287

U

Uninstall
about 486
procedure 486
unknown viruses 407
updates
automatically 57
checking 55
obtaining 59
Pulse Updates 59
summary 50
upgrading
new version 474
User-Specified Programs
about 174
adding programs 174
Quiet Mode 174
removing programs 175

V

version number
checking 473
virus protection
about 407
system scans 118
updates 407
viruses
automatic protection 407
descriptions 407
unknown 407
Vulnerability Protection
about 251, 253
viewing programs 252

W

Web pages
launching 338
protection 302
reporting 304
Web Query
about 267
turning off 268
turning on 268
Web Settings
about 444
wireless network
viewing status 294
Worm Blocking
threats found by 186
worms
found by Worm Blocking 186
in email messages 186

Norton from Symantec products protect consumers from traditional threats with antivirus, antispam, and Spyware Protection. They also protect against bots, drive-by downloads, and identity theft, and are light on system resources. In addition, Symantec provides services such as online backup and PC Tuneup, and is a trusted source for family online safety. For more information, please click one of the following links:

Antivirus | Antispam | Spyware Protection | Online Backup

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, Norton, and the Norton Logo are trademarks or registered trademarks of Symantec Corporation and its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.